SERIE GENERALE

Spediz. abb. post. - art. 1, comma 1
Legge 27-02-2004, n. 46 - Filiale di Roma

Anno 165° - Numero 230

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA **Roma - Martedì, 1° ottobre 2024** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA, 70 - 00186 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - VIA SALARIA, 691 - 00138 ROMA - CENTRALINO 06-85081 - LIBRERIA DELLO STATO PIAZZA G. VERDI, 1 - 00198 ROMA

La **Gazzetta Ufficiale, Parte Prima,** *oltre alla* **Serie Generale**, *pubblica cinque Serie speciali, ciascuna contraddistinta da autonoma numerazione:*

- **1ª Serie speciale:** *Corte costituzionale (pubblicata il mercoledì)*
- **2ª Serie speciale:** *Unione europea (pubblicata il lunedì e il giovedì)*
- **3ª Serie speciale:** *Regioni (pubblicata il sabato)*
- **4ª Serie speciale:** *Concorsi ed esami (pubblicata il martedì e il venerdì)*
- **5ª Serie speciale:** *Contratti pubblici (pubblicata il lunedì, il mercoledì e il venerdì)*

La **Gazzetta Ufficiale, Parte Seconda,** "Foglio delle inserzioni", *è pubblicata il martedì, il giovedì e il sabato*

AVVISO ALLE AMMINISTRAZIONI

Al fine di ottimizzare la procedura di pubblicazione degli atti in *Gazzetta Ufficiale,* le Amministrazioni sono pregate di inviare, contemporaneamente e parallelamente alla trasmissione su carta, come da norma, anche copia telematica dei medesimi (in formato word) al seguente indirizzo di posta elettronica certificata: gazzettaufficiale@giustiziacert.it, curando che, nella nota cartacea di trasmissione, siano chiaramente riportati gli estremi dell'invio telematico (mittente, oggetto e data).

Nel caso non si disponga ancora di PEC, e fino all'adozione della stessa, sarà possibile trasmettere gli atti a: gazzettaufficiale@giustizia.it

SOMMARIO

LEGGI ED ALTRI ATTI NORMATIVI

DECRETO-LEGGE 1° ottobre 2024, n. **137**.

Misure urgenti per contrastare i fenomeni di violenza nei confronti dei professionisti sanitari, socio-sanitari, ausiliari e di assistenza e cura nell'esercizio delle loro funzioni nonché di danneggiamento dei beni destinati all'assistenza sanitaria. (24G00158) . . . . *Pag.* 1

DECRETO LEGISLATIVO 4 settembre 2024, n. **138**.

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. (24G00155). . . . . *Pag.* 2

ATTI DEGLI ORGANI COSTITUZIONALI

Camera dei deputati

Convocazione del Parlamento in seduta comune. (24A05227) . . . . *Pag.* 59

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

Ministero dell'agricoltura, della sovranità alimentare e delle foreste

DECRETO 6 settembre 2024.

Riconoscimento dell'idoneità al Centro di saggio «Agroservice R&S s.r.l.» ad effettuare prove ufficiali di campo, finalizzate alla produzione di dati di efficacia e alla determinazione dell'entità dei residui di prodotti fitosanitari. (24A05071). *Pag.* 59

DECRETO 6 settembre 2024.

Riconoscimento dell'idoneità al Centro di saggio «Bayer CropScience s.r.l.» ad effettuare prove ufficiali di campo, finalizzate alla produzione di dati di efficacia e alla determinazione dell'entità dei residui di prodotti fitosanitari. (24A05072). *Pag.* 61

Ministero dell'economia e delle finanze

DECRETO 26 settembre 2024.

Emissione dei buoni ordinari del Tesoro a 182 giorni, prima e seconda *tranche.* (24A05110) . . *Pag.* 63

DECRETO 27 settembre 2024.

Riapertura delle operazioni di sottoscrizione dei buoni del Tesoro poliennali 3,00%, con godimento 1° febbraio 2019 e scadenza 1° agosto 2029, diciassettesima e diciottesima *tranche*. (24A05138) . . . . *Pag.* 66

DECRETO 27 settembre 2024.

Riapertura delle operazioni di sottoscrizione dei buoni del Tesoro poliennali 3,85%, con godimento 1° agosto 2024 e scadenza 1° febbraio 2035, quinta e sesta *tranche*. (24A05139) . . . . . . *Pag.* 68

DECRETI E DELIBERE DI ALTRE AUTORITÀ

Comitato interministeriale per la programmazione economica e lo sviluppo sostenibile

DELIBERA 9 luglio 2024.

Nuclei di valutazione e verifica degli investimenti pubblici. Ripartizione risorse anno 2024 (articolo 1, comma 7, della legge n. 144/1999). (Delibera n. 50/2024). (24A05073) . . . . *Pag.* 70

ESTRATTI, SUNTI E COMUNICATI

Agenzia italiana del farmaco

Autorizzazione all'immissione in commercio del medicinale per uso umano, a base di dorzolamide cloridrato e timololo maleato, «Dorzolamide Timololo Omnivision». (24A05011) . . . . *Pag.* 74

Autorizzazione all'immissione in commercio del medicinale per uso umano, a base di ciclopentolato cloridrato, «Plegik». (24A05012) . . . . *Pag.* 75

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di clotrimazolo, «Clozol». (24A05014) . . . . *Pag.* 76

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di meropenem, «Merrem». (24A05015) . . . . *Pag.* 76

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di destrometorfano bromidrato, «Vicks Tosse Sedativo». (24A05016) . . . . *Pag.* 77

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di estratto secco di cimicifuga recamosa (L.) Nutt., rhizoma, «Cimifemin». (24A05033) . . . . *Pag.* 77

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di [18F] PSMA-1007, «Radelumin». (24A05053) . . *Pag.* 77

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di [18F] PSMA-1007, «Radelumin». (24A05054) . . *Pag.* 78

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di acido folico, «Acido folico Aristo». (24A05055) . *Pag.* 79

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di itraconazolo, «Itragerm». (24A05056) . . . . *Pag.* 80

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di citisiniclina «Kobayzaren». (24A05057). . . . . *Pag.* 80

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di Tiapride cloridrato, «Italprid». (24A05058) . . . . . *Pag.* 81

Revoca, su rinuncia, dell'autorizzazione all'immissione in commercio di taluni medicinali per uso umano (24A05059) . . . . *Pag.* 81

Revoca, su rinuncia, dell'autorizzazione all'importazione parallela del medicinale per uso umano «Ananase». (24A05060) . . . . *Pag.* 81

Ministero dell'agricoltura, della sovranità alimentare e delle foreste

Modalità di presentazione e contenuti della domanda di iscrizione di varietà e cloni di vite al Registro nazionale. Abrogazione decreto 30 settembre 2021. (24A05074) . . . . *Pag.* 81

Ministero dell'ambiente e della sicurezza energetica

Invito alla manifestazione di interesse per la redazione di pareri sulla verifica della capacità economico-finanziaria degli operatori del settore energetico e/o minerario e per il relativo posizionamento ai fini del rilascio e della gestione dei titoli e delle autorizzazioni conferite nei predetti settori. (24A05075). *Pag.* 82

Ministero delle imprese e del made in Italy

Ripartizione delle risorse residue disponibili in attuazione dell'articolo 6, comma 2, del decreto 3 giugno 2024, per il riconoscimento, per l'anno 2024, del contributo per l'installazione di impianti nuovi a GPL o a metano per l'autotrazione su veicoli di categoria M1 omologati. (24A05100) . . . . . . *Pag.* 82

LEGGI ED ALTRI ATTI NORMATIVI

DECRETO-LEGGE 1° ottobre 2024, n. **137**.

Misure urgenti per contrastare i fenomeni di violenza nei confronti dei professionisti sanitari, socio-sanitari, ausiliari e di assistenza e cura nell'esercizio delle loro funzioni nonché di danneggiamento dei beni destinati all'assistenza sanitaria.

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 77 e 87, quinto comma, della Costituzione;

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri» e, in particolare, l'articolo 15;

Vista la legge 14 agosto 2020, n. 113, recante «Disposizioni in materia di sicurezza per gli esercenti le professioni sanitarie e socio-sanitarie nell'esercizio delle loro funzioni»;

Visto il decreto-legge 30 marzo 2023, n. 34, convertito, con modificazioni, dalla legge 26 maggio 2023, n. 56, recante «Misure urgenti a sostegno delle famiglie e delle imprese per l'acquisto di energia elettrica e gas naturale, nonché in materia di salute e adempimenti fiscali» e, in particolare, l'articolo 16, che prevede disposizioni in materia di contrasto degli atti di violenza nei confronti del personale sanitario;

Visto il decreto legislativo 19 marzo 2024, n. 31, recante «Disposizioni integrative e correttive del decreto legislativo 10 ottobre 2022, n. 150, di attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari»;

Ritenuta la straordinaria necessità e urgenza, attesa la recrudescenza di gravi episodi di violenza in danno dei professionisti e delle strutture sanitarie pubbliche, in particolare nei pronto soccorso, di adottare misure idonee a costituire un valido ed effettivo apparato di deterrenza e contrasto a tali episodi che colpiscono e mortificano il personale addetto a tali delicate funzioni e rischiano di depauperare il patrimonio sanitario pubblico;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 27 settembre 2024;

Sulla proposta del Presidente del Consiglio dei ministri, dei Ministri della salute e della giustizia, di concerto con il Ministro dell'interno;

EMANA
il seguente decreto-legge:

Art. 1.

Modifiche all'articolo 635 del codice penale

1. All'articolo 635 del codice penale, dopo il secondo comma è inserito il seguente:

«Chiunque, all'interno o nelle pertinenze di strutture sanitarie o socio-sanitarie residenziali o semiresidenziali, pubbliche o private, con violenza alla persona o con minaccia ovvero in occasione del delitto previsto dall'articolo 583-*quater*, distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose ivi esistenti o comunque destinate al servizio sanitario o socio-sanitario, è punito con la reclusione da uno a cinque anni e con la multa fino a 10.000 euro. Se il fatto è commesso da più persone riunite, la pena è aumentata.».

Art. 2.

Modifiche agli articoli 380 e 382-bis *del codice di procedura penale*

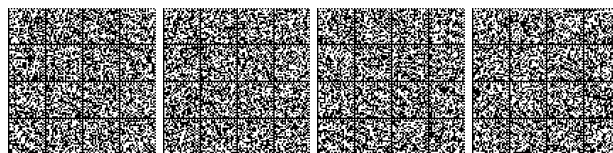
1. Al codice di procedura penale sono apportate le seguenti modificazioni:

a) all'articolo 380, comma 2, dopo la lettera a-*bis*) sono inserite le seguenti:

«a-*ter*) delitto di lesioni personali a personale esercente una professione sanitaria o socio-sanitaria e a chiunque svolga attività ausiliarie ad essa funzionali previsto dall'articolo 583-*quater*, secondo comma, del codice penale;

a-*quater*) delitto di danneggiamento previsto dall'articolo 635, terzo comma, del codice penale;»;

b) all'articolo 382-*bis*, dopo il comma 1 è aggiunto il seguente:

«1-*bis*. Nei casi di delitti non colposi per i quali è previsto l'arresto in flagranza, commessi all'interno o nelle pertinenze delle strutture sanitarie o socio-sanitarie residenziali o semiresidenziali, pubbliche o private, in danno di persone esercenti una professione sanitaria o socio-sanitaria nell'esercizio o a causa delle funzioni o del servizio nonché di chiunque svolga attività ausiliarie di cura, assistenza sanitaria o soccorso, funzionali allo svolgimento di dette professioni, nell'esercizio o a causa di tali attività, ovvero commessi su cose ivi esistenti o comunque destinate al servizio sanitario o socio-sanitario, quando non è possibile procedere immediatamente all'arresto per ragioni di sicurezza o incolumità pubblica o individuale ovvero per ragioni inerenti alla regolare erogazione del servizio, si considera comunque in stato di flagranza ai sensi dell'articolo 382 colui il quale, sulla base di documentazione video-fotografica o di altra documentazione legittimamente ottenuta da dispositivi di comunicazione informatica o telematica, dalla quale emerga inequivocabilmente il fatto, ne risulta autore, sempre che

l'arresto sia compiuto non oltre il tempo necessario alla sua identificazione e, comunque, entro le quarantotto ore dal fatto.».

Art. 3.

Clausola di invarianza finanziaria

1. Dall'attuazione delle disposizioni di cui al presente decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni e le autorità interessate provvedono alle attività ivi previste nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Art. 4.

Entrata in vigore

1. Il presente decreto entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana e sarà presentato alle Camere per la conversione in legge.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 1° ottobre 2024

MATTARELLA

MELONI, *Presidente del Consiglio dei ministri*

SCHILLACI, *Ministro della salute*

NORDIO, *Ministro della giustizia*

PIANTEDOSI, *Ministro dell'interno*

Visto, *il Guardasigilli:* NORDIO

24G00158

DECRETO LEGISLATIVO 4 settembre 2024, n. **138**.

Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148.

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87, quinto comma, della Costituzione;

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri» e, in particolare, l'articolo 14;

Vista la legge 24 dicembre 2012, n. 234, recante «Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea» e, in particolare, gli articoli 31 e 32;

Vista la legge 21 febbraio 2024, n. 15, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea - Legge di delegazione europea 2022-2023» e, in particolare, l'articolo 3;

Vista la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;

Vista la comunicazione della Commissione, del 13 settembre 2023, relativa all'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva (UE) 2022/2555;

Vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche);

Visto il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;

Visto il regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale;

Visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»);

Vista la raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese;

Vista la direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio;

Visto il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011;

Vista la direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario;

Vista la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE»;

Visto il decreto legislativo 1° agosto 2003, n. 259, recante «Codice delle comunicazioni elettroniche»;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale» e, in particolare, le disposizioni in materia di funzioni dell'AgID e di sicurezza informatica;

Visto il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, recante «Misure urgenti per il contrasto del terrorismo internazionale»;

Vista la legge 3 agosto 2007, n. 124, recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto»;

Visto il decreto legislativo 23 giugno 2011, n. 118, recante «Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42»;

Visto il decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, recante «Misure urgenti per la crescita del Paese» e, in particolare, l'articolo 19, che ha istituito l'Agenzia per l'Italia digitale (AgID);

Visto il decreto legislativo 4 marzo 2014, n. 39, recante «Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI»;

Visto il decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, recante «Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione»;

Visto il decreto legislativo 18 maggio 2018, n. 65, recante «Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione»;

Visto il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica»;

Visto il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»;

Vista la legge 28 giugno 2024, n. 90, recante «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici»;

Visto il decreto legislativo adottato ai sensi dell'articolo 5 della legge n. 15 del 2024 per il recepimento della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio;

Visto il decreto del Presidente del Consiglio dei ministri n. 5 del 6 novembre 2015, recante «Disposizioni per la tutela amministrativa del segreto di Stato e delle informazioni classificate e a diffusione esclusiva», pubblicato nella *Gazzetta Ufficiale* n. 284 del 5 dicembre 2015;

Visto il decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, concernente «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali», pubblicato nella *Gazzetta Ufficiale* n. 87 del 13 aprile 2017;

Sentita l'Agenzia per la cybersicurezza nazionale, ai sensi dell'articolo 3 della legge n. 15 del 2024;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 10 giugno 2024;

Acquisito il parere della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, reso nella seduta dell'11 luglio 2024

Acquisiti i pareri delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del 7 agosto 2024;

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro per gli affari europei, il Sud, le politiche di coesione e il PNRR, di concerto con i Ministri per la pubblica amministrazione, degli affari esteri e della cooperazione internazionale, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, delle imprese e del made in Italy, dell'agricoltura, della sovranità alimentare e delle foreste, dell'ambiente e della sicurezza energetica, delle infrastrutture e dei trasporti, dell'università e della ricerca, della cultura e della salute;

EMANA
il seguente decreto legislativo:

Capo I
DISPOSIZIONI GENERALI

Art. 1.
Oggetto

1. Il presente decreto stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea in modo da migliorare il funzionamento del mercato interno.

2. Ai fini del comma 1, il presente decreto prevede:

a) la Strategia nazionale di cybersicurezza, recante previsioni volte a garantire un livello elevato di sicurezza informatica;

b) l'integrazione del quadro di gestione delle crisi informatiche, nel contesto dell'organizzazione nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza, di cui all'articolo 10 del decreto-legge 4 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

c) la conferma dell'Agenzia per la cybersicurezza nazionale quale:

1) Autorità nazionale competente NIS, disciplinandone i poteri inerenti all'implementazione e all'attuazione del presente decreto;

2) Punto di contatto unico NIS, assicurando il raccordo nazionale e transfrontaliero;

3) Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT Italia);

d) la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del Ministero della difesa, ciascuno per gli ambiti di competenza indicati all'articolo 2, comma 1, lettera *g)*, quali Autorità nazionali di gestione delle crisi informatiche su vasta scala, assicurando la coerenza con il quadro nazionale esistente in materia di gestione generale delle crisi informatiche, fermi restando i compiti del Nucleo per la cybersicurezza di cui all'articolo 9 del decreto-legge 14 giugno 2021, n. 82;

e) l'individuazione di Autorità di settore NIS che collaborano con l'Agenzia per la cybersicurezza nazionale, supportandone le funzioni svolte quale Autorità nazionale competente NIS e Punto di contatto unico NIS;

f) l'indicazione dei criteri per l'individuazione dei soggetti a cui si applica il presente decreto e la definizione dei relativi obblighi in materia di misure di gestione dei rischi per la sicurezza informatica e di notifica di incidente;

g) l'adozione di misure in materia di cooperazione e di condivisione delle informazioni ai fini dell'applicazione del presente decreto, in particolare, attraverso la partecipazione nazionale a livello dell'Unione europea:

1) al Gruppo di cooperazione NIS tra autorità competenti NIS e tra punti di contatto unici degli Stati membri dell'Unione europea, nell'ottica di incrementare la fiducia e la collaborazione a livello unionale;

2) alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi cibernetiche su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione europea;

3) alla Rete di CSIRT nazionali nell'ottica di assicurare una cooperazione, sul piano tecnico, rapida ed efficace.

Art. 2.

Definizioni

1. Ai fini del presente decreto si applicano le definizioni seguenti:

a) «Strategia nazionale di cybersicurezza»: il quadro coerente che prevede gli obiettivi strategici e le priorità in materia di cybersicurezza, nonché la governance per il loro conseguimento, di cui all'articolo 9;

b) «Agenzia per la cybersicurezza nazionale»: l'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, comma 1, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

c) «Nucleo per la cybersicurezza»: il Nucleo per la cybersicurezza di cui all'articolo 8 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

d) «Autorità nazionale competente NIS»: l'Agenzia per la cybersicurezza nazionale, quale Autorità nazionale competente NIS di cui all'articolo 10, comma 1;

e) «Punto di contatto unico NIS»: l'Agenzia per la cybersicurezza nazionale, quale Punto di contatto unico NIS di cui all'articolo 10, comma 2;

f) «Autorità di settore NIS»: le Amministrazioni designate quali Autorità di settore di cui all'articolo 11, commi 1 e 2;

g) «Autorità nazionali di gestione delle crisi informatiche»: per la parte relativa alla resilienza nazionale di cui all'articolo 1 del decreto-legge n. 82 del 2021, l'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e, per la parte relativa alla difesa dello Stato, il Ministero della difesa, quali Autorità nazionali responsabili della gestione degli incidenti e delle crisi di cybersicurezza su vasta scala, di cui all'articolo 9 della direttiva (UE) 2022/2555;

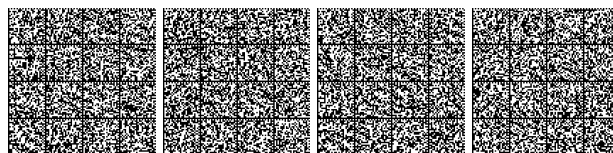
h) «CSIRT nazionali»: i Gruppi nazionali di risposta agli incidenti di sicurezza informatica di cui all'articolo 10, paragrafo 1, della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

i) «CSIRT Italia»: il Gruppo nazionale di risposta agli incidenti di sicurezza informatica ai sensi dell'articolo 15, comma 1, operante all'interno dell'Agenzia per la cybersicurezza nazionale;

l) «Gruppo di cooperazione NIS»: il Gruppo di cooperazione di cui all'articolo 18, istituito ai sensi dell'articolo 14 della direttiva (UE) 2022/2555;

m) «EU-CyCLONe»: la Rete delle organizzazioni di collegamento per le crisi informatiche di cui all'articolo 19, istituita ai sensi dell'articolo 16 della direttiva (UE) 2022/2555;

n) «Rete di CSIRT nazionali»: la Rete di CSIRT nazionali di cui all'articolo 20, istituita ai sensi dell'articolo 15 della direttiva (UE) 2022/2555;

o) «ENISA»: l'Agenzia dell'Unione europea per la sicurezza informatica, di cui all'articolo 3 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019;

p) «sistema informativo e di rete»:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera *vv)*, del decreto legislativo 1° agosto 2003, n. 259;

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;

q) «sicurezza dei sistemi informativi e di rete»: la capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi;

r) «sicurezza informatica»: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche, così come definito dall'articolo 2, punto 1), del regolamento (UE) 2019/881;

s) «cybersicurezza»: ferme restando le definizioni di cui alle lettere *q)* e *r)*, l'insieme delle attività di cui all'articolo 1, comma 1, lettera *a)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109;

t) «incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;

u) «quasi-incidente»: cd. *near-miss*, un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato;

v) «incidente di sicurezza informatica su vasta scala»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri;

z) «gestione degli incidenti»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e recuperare da esso;

aa) «rischio»: la combinazione dell'entità dell'impatto di un incidente, in termini di danno o di perturbazione, e della probabilità che quest'ultimo si verifichi;

bb) «minaccia informatica»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone, così come definita dall'articolo 2, punto 8), del regolamento (UE) 2019/881;

cc) «minaccia informatica significativa»: una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informativi e di rete di un soggetto o sugli utenti dei servizi erogati da un soggetto causando perdite materiali o immateriali considerevoli;

dd) «approccio multi-rischio»: cosiddetto approccio *all-hazards*, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati;

ee) «singoli punti di malfunzionamento»: cosiddetto *single points of failure*, singolo componente di un sistema da cui dipende il funzionamento del sistema stesso;

ff) «prodotto TIC»: un elemento o un gruppo di elementi di un sistema informativo o di rete, così come definito dall'articolo 2, punto 12), del regolamento (UE) 2019/881;

gg) «servizio TIC»: un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo dei sistemi informativi e di rete così come definito dall'articolo 2, punto 13), del regolamento (UE) 2019/881;

hh) «processo TIC»: un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto TIC o servizio TIC, così come definito dall'articolo 2, punto 14), del regolamento (UE) 2019/881;

ii) «vulnerabilità»: un punto debole, una suscettibilità o un difetto di prodotti TIC o servizi TIC che può essere sfruttato da una minaccia informatica;

ll) «specifica tecnica»: una specifica tecnica quale definita all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012;

mm) «punto di interscambio internet»: cosiddetto *internet exchange point* (IXP), un'infrastruttura di rete che consente l'interconnessione di più di due reti indipendenti (sistemi autonomi), principalmente al fine di agevolare lo scambio del traffico internet, che fornisce interconnessione soltanto ai sistemi autonomi e che non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo né altera o interferisce altrimenti con tale traffico;

nn) «sistema dei nomi di dominio»: cosiddetto *domain name system* (DNS), un sistema di nomi gerarchico e distribuito che consente l'identificazione di servizi e risorse su internet, permettendo ai dispositivi degli utenti finali di utilizzare i servizi di instradamento e connettività di internet al fine di accedere a tali servizi e risorse;

oo) «fornitore di servizi di sistema dei nomi di dominio»: un soggetto che fornisce alternativamente:

1) servizi di risoluzione dei nomi di dominio ricorsivi accessibili al pubblico per gli utenti finali di internet;

2) servizi di risoluzione dei nomi di dominio autoritativi per uso da parte di terzi, fatta eccezione per i server dei nomi radice (cosiddetto *root nameserver*);

pp) «gestore di registro dei nomi di dominio di primo livello»: cosiddetto registro dei nomi TLD (*top level domain*) o *registry*, soggetto cui è stato delegato uno specifico dominio di primo livello e che è responsabile

dell'amministrazione di tale dominio di primo livello, compresa la registrazione dei nomi di dominio sotto tale dominio di primo livello, e del funzionamento tecnico di tale dominio di primo livello, compresi il funzionamento dei server dei nomi, la manutenzione delle banche dati e la distribuzione dei file di zona del dominio di primo livello tra i server dei nomi, indipendentemente dal fatto che una qualsiasi di tali operazioni sia effettuata dal soggetto stesso o sia esternalizzata, ma escludendo le situazioni in cui i nomi di dominio di primo livello sono utilizzati da un registro esclusivamente per uso proprio;

qq) «fornitore di servizi di registrazione di nomi di dominio»: un *registrar* o un agente che agisce per conto di *registrar*, come un fornitore o un rivenditore di servizi di registrazione per la privacy o di proxy;

rr) «servizio digitale»: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi, quale definito all'articolo 1, paragrafo 1, lettera *b)*, della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015;

ss) «servizio fiduciario»: un servizio fiduciario quale definito all'articolo 3, punto 16), del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2024;

tt) «prestatore di servizi fiduciari»: una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato, quale definito all'articolo 3, punto 19), del regolamento (UE) n. 910/2014;

uu) «servizio fiduciario qualificato»: un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel regolamento (UE) n. 910/2014, ai sensi dell'articolo 3, punto 17) dello stesso;

vv) «prestatore di servizi fiduciari qualificato»: un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato, quale definito all'articolo 3, punto 20), del regolamento (UE) n. 910/2014;

zz) «mercato online»: un servizio che utilizza un software, compresi siti web, parte di siti web o un'applicazione, gestito da o per conto del professionista, che permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori, quale definito all'articolo 2, lettera *n)*, della direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005;

aaa) «motore di ricerca online»: un servizio digitale che consente all'utente di formulare domande al fine di effettuare ricerche, in linea di principio, su tutti i siti web, o su tutti i siti web in una lingua particolare, sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, richiesta vocale, frase o di altro input, e che restituisce i risultati in qualsiasi formato in cui possono essere trovate le informazioni relative al contenuto richiesto, quale definito all'articolo 2, punto 5), del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio, del 20 giugno 2019;

bbb) «servizio di cloud computing»: un servizio digitale che consente l'amministrazione su richiesta di un *pool* scalabile ed elastico di risorse di calcolo condivisibili e l'ampio accesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni;

ccc) «servizio di data center»: un servizio che comprende strutture, o gruppi di strutture, dedicate a ospitare in modo centralizzato, interconnettere e far funzionare apparecchiature informatiche e di rete che forniscono servizi di conservazione, elaborazione e trasporto di dati insieme a tutti gli impianti e le infrastrutture per la distribuzione dell'energia e il controllo ambientale;

ddd) «rete di distribuzione dei contenuti»: cosiddetta *content delivery network* (CDN), una rete di server distribuiti geograficamente allo scopo di garantire l'elevata disponibilità, l'accessibilità o la rapida distribuzione di contenuti e servizi digitali agli utenti di internet per conto di fornitori di contenuti e servizi;

eee) «piattaforma di servizi di social network»: una piattaforma che consente agli utenti finali di entrare in contatto, condividere, scoprire e comunicare gli uni con gli altri su molteplici dispositivi, in particolare, attraverso chat, post, video e raccomandazioni;

fff) «rete pubblica di comunicazione elettronica»: una rete di comunicazione elettronica, utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di rete, quale definita all'articolo 2, punto 8), della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018;

ggg) «servizio di comunicazione elettronica»: un servizio di comunicazione elettronica quale definito all'articolo 2, punto 4), della direttiva (UE) 2018/1972;

hhh) «soggetto»: una persona fisica o giuridica, costituita e riconosciuta come tale conformemente al diritto nazionale applicabile nel suo luogo di stabilimento, che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi;

iii) «fornitore di servizi gestiti»: un soggetto che fornisce servizi relativi all'installazione, alla gestione, al funzionamento o alla manutenzione di prodotti, reti, infrastrutture, applicazioni TIC o di qualsiasi altro sistema informativo e di rete, tramite assistenza o amministrazione attiva effettuata nei locali dei clienti o a distanza;

lll) «fornitore di servizi di sicurezza gestiti»: un fornitore di servizi gestiti che svolge o fornisce assistenza per attività relative alla gestione dei rischi di sicurezza informatica;

mmm) «organismo di ricerca»: un soggetto che ha come obiettivo principale lo svolgimento di attività di ricerca applicata o di sviluppo sperimentale al fine di sfruttare i risultati di tale ricerca a fini commerciali, ma che non comprende gli istituti di istruzione;

nnn) «audit»: attività di verifica, a distanza o in loco, sistematica, documentata e indipendente che ha come scopo quello di vagliare la corrispondenza agli obblighi di cui al capo IV del presente decreto, effettuata da un organismo indipendente qualificato o dall'Autorità nazionale competente NIS.

Art. 3.

Ambito di applicazione

1. Nell'ambito di applicazione del presente decreto rientrano i soggetti pubblici e privati delle tipologie di cui agli allegati I, II, III e IV, che costituiscono parte integrante del presente decreto, che sono sottoposti alla giurisdizione nazionale ai sensi dell'articolo 5. Gli allegati I e II descrivono i settori ritenuti, rispettivamente, altamente critici e critici, nonché i relativi sottosettori e le tipologie di soggetti. Gli allegati III e IV descrivono, rispettivamente, le categorie di pubbliche amministrazioni e le ulteriori tipologie di soggetto a cui si applica il presente decreto.

2. Il presente decreto si applica ai soggetti delle tipologie di cui all'allegato I e II, che superano i massimali per le piccole imprese ai sensi dell'articolo 2, paragrafo 2, dell'allegato alla raccomandazione 2003/361/CE.

3. L'articolo 3, paragrafo 4, dell'allegato alla raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, non si applica ai fini del presente decreto.

4. Per determinare se un soggetto è da considerarsi una media o grande impresa ai sensi dell'articolo 2 dell'allegato della raccomandazione 2003/361/CE, si applica l'articolo 6, paragrafo 2, del medesimo allegato, salvo che ciò non sia proporzionato, tenuto anche conto dell'indipendenza del soggetto dalle sue imprese collegate in termini di sistemi informativi e di rete che utilizza nella fornitura dei suoi servizi e in termini di servizi che fornisce.

5. Il presente decreto si applica, indipendentemente dalle loro dimensioni, anche:

a) ai soggetti che sono identificati come soggetti critici ai sensi del decreto legislativo, che recepisce la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

b) ai fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico;

c) ai prestatori di servizi fiduciari;

d) ai gestori di registri dei nomi di dominio di primo livello e fornitori di servizi di sistema dei nomi di dominio;

e) ai fornitori di servizi di registrazione dei nomi di dominio.

6. Il presente decreto si applica, altresì, anche indipendentemente dalle loro dimensioni, alle pubbliche amministrazioni di cui all'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ricomprese nelle categorie elencate nell'allegato III.

7. Sulla base di un criterio di gradualità, dell'evoluzione del grado di esposizione al rischio della pubblica amministrazione, della probabilità che si verifichino incidenti e della loro gravità, compreso il loro impatto sociale ed economico, tenuto conto anche dei criteri di cui al comma 9, con uno o più decreti del Presidente del Consiglio dei ministri adottati secondo le modalità di cui all'articolo 40, comma 2, possono essere individuate ulteriori categorie di pubbliche amministrazioni a cui si applica il presente decreto al fine di adeguare l'elenco di categorie di cui all'allegato III.

8. Il presente decreto si applica, altresì, indipendentemente dalle loro dimensioni, anche ai soggetti delle tipologie di cui all'allegato IV, individuati secondo le procedure di cui al comma 13.

9. Il presente decreto si applica, altresì, anche ai soggetti dei settori o delle tipologie di cui agli allegati I, II, III e IV, indipendentemente dalle loro dimensioni, individuati secondo le procedure di cui al comma 13, qualora:

a) il soggetto sia identificato prima della data di entrata in vigore del presente decreto come operatore di servizi essenziali ai sensi del decreto legislativo 18 maggio 2018, n. 65;

b) il soggetto sia l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;

c) una perturbazione del servizio fornito dal soggetto potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;

d) una perturbazione del servizio fornito dal soggetto potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;

e) il soggetto sia critico in ragione della sua particolare importanza a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nel territorio dello Stato;

f) il soggetto sia considerato critico ai sensi del presente decreto quale elemento sistemico della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti.

10. Il presente decreto si applica, infine, indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri:

a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;

b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;

c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale;

d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

11. Resta ferma la disciplina in materia di protezione dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e al decreto legislativo 30 giugno 2003, n. 196, nonché in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile di cui al decreto legislativo 4 marzo 2014, n. 39.

12. L'Autorità nazionale competente NIS applica la clausola di salvaguardia di cui al comma 4, secondo i criteri per la determinazione individuati con le modalità di cui all'articolo 40, comma 1.

13. I soggetti di cui ai commi 8 e 9 sono individuati dall'Autorità nazionale competente NIS, su proposta delle Autorità di settore, secondo le modalità di cui all'arti-

colo 40, comma 4. L'Autorità nazionale competente NIS notifica a tali soggetti la loro individuazione ai fini della registrazione di cui all'articolo 7, comma 1.

14. Le disposizioni di cui all'articolo 17 e ai Capi IV e V del presente decreto non si applicano ai soggetti identificati come essenziali o importanti dei settori 3 e 4 di cui all'allegato I, ai quali si applica la disciplina di cui al regolamento (UE) 2022/2554.

15. Il presente decreto non si applica, ai sensi dell'articolo 2, comma 10, della direttiva, ai soggetti esentati dall'ambito di applicazione del regolamento (UE) 2022/2554.

Art. 4.

Protezione degli interessi nazionali e commerciali

1. Il presente decreto lascia impregiudicata la responsabilità dello Stato italiano di tutelare la sicurezza nazionale e il suo potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico.

2. I soggetti di cui all'articolo 3, commi 6 e 7, non ricomprendono il Parlamento italiano, l'Autorità giudiziaria, la Banca d'Italia e l'Unità di informazione finanziaria per l'Italia di cui all'articolo 6 del decreto legislativo 21 novembre 2007, n. 231. Agli Organi costituzionali e di rilievo costituzionale non si applicano le previsioni di cui al capo V.

3. Il presente decreto non si applica agli enti, organi e articolazioni della pubblica amministrazione che operano nei settori della pubblica sicurezza, della difesa nazionale, o dell'attività di contrasto, compresi l'indagine, l' accertamento e il perseguimento di reati, nonché agli organismi di informazione per la sicurezza di cui alla legge 3 agosto 2007, n. 124, all'Agenzia per la cybersicurezza nazionale di cui al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109.

4. Fermo restando quanto previsto dal comma 3, con uno o più decreti del Presidente del Consiglio dei ministri adottati, anche su proposta dei Ministri della giustizia, dell'interno e della difesa, per gli ambiti di rispettiva competenza, d'intesa con l'Agenzia per la cybersicurezza nazionale, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli enti, organi e articolazioni della pubblica amministrazione di cui al comma 3, nonché in materia di protezione civile. A tali soggetti, nell'espletamento di tali attività o servizi, non si applicano gli obblighi di cui al capo IV e le previsioni di cui al capo V.

5. Con decreto del Presidente del Consiglio dei ministri, adottato ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, sono individuati i soggetti che svolgono attività o forniscono servizi in via esclusiva per gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007. A tali soggetti, nell'espletamento dei predetti attività o servizi, non si applicano gli obblighi di cui al capo IV e le previsioni di cui al capo V. Dei provvedimenti adottati ai sensi del primo periodo viene data comunicazione all'Agenzia per la cybersicurezza nazionale.

6. Ai sensi del comma 4, non possono essere esclusi gli enti, organi e articolazioni della pubblica amministrazione con competenze di regolazione o le cui attività sono solo marginalmente connesse ai settori di cui al medesimo comma. Non possono altresì essere esclusi i soggetti che agiscono in qualità di prestatore di servizi fiduciari. I soggetti di cui al comma 4 assicurano un livello di sicurezza informatica coerente con gli obblighi di cui al capo IV.

7. Gli obblighi stabiliti nel presente decreto non comportano la fornitura di informazioni la cui divulgazione sia contraria agli interessi essenziali dello Stato italiano in materia di sicurezza nazionale, pubblica sicurezza o difesa.

8. Fatto salvo quanto previsto dall'articolo 346 del trattato sul funzionamento dell'Unione europea, le informazioni riservate secondo quanto disposto dalla normativa dell'Unione europea e nazionale, in particolare per quanto concerne la riservatezza degli affari, sono scambiate con la Commissione europea e con le autorità competenti degli Stati membri solo nella misura in cui tale scambio sia necessario ai fini dell'applicazione del presente decreto. Le informazioni scambiate sono pertinenti e commisurate allo scopo. Lo scambio di informazioni ne tutela la riservatezza e protegge la sicurezza e gli interessi commerciali dei soggetti essenziali e dei soggetti importanti.

Art. 5.

Giurisdizione e territorialità

1. Sono sottoposti alla giurisdizione nazionale i soggetti di cui all'articolo 3 stabiliti sul territorio nazionale, ad eccezione dei seguenti casi:

a) i fornitori di reti pubbliche di comunicazione elettronica o i fornitori di servizi di comunicazione elettronica accessibili al pubblico, che sono considerati sotto la giurisdizione dello Stato membro nel quale forniscono i loro servizi;

b) i fornitori di servizi di sistema dei nomi di dominio DNS, i registri dei nomi di dominio di primo livello, i soggetti che forniscono servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online o di piattaforme di servizi di social network, che sono sottoposti la giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione ai sensi del comma 2;

c) gli enti della pubblica amministrazione, che sono sottoposti alla giurisdizione dello Stato membro che li ha istituiti.

2. Ai fini di cui al comma 1, lettera *b)*, si considera stabilimento principale nell'Unione quello dello Stato membro nel quale sono prevalentemente adottate le decisioni relative alle misure di gestione del rischio per la sicurezza informatica. Se non è possibile determinare lo Stato membro in cui sono adottate le suddette decisioni o se le stesse non sono adottate nell'Unione, lo stabilimento principale è considerato quello collocato nello Stato membro in cui sono effettuate le operazioni di sicurezza

informatica, ovvero, ove ciò non sia possibile, quello dello Stato membro in cui il soggetto interessato ha lo stabilimento con il maggior numero di dipendenti nell'Unione europea.

3. Se i soggetti di cui al comma 1, lettera *b)*, non sono stabiliti nel territorio dell'Unione ma offrono servizi all'interno dello stesso, essi designano un rappresentante nell'Unione, che è stabilito in uno degli Stati membri in cui sono offerti i predetti servizi ed è sottoposto alla relativa giurisdizione.

4. In assenza della designazione del rappresentante da parte di uno dei soggetti di cui al comma 3, l'Autorità nazionale competente NIS può avviare un'azione legale, nei confronti dei soggetti inadempienti.

5. La designazione del rappresentante di cui al comma 3 non pregiudica le azioni legali che potrebbero essere state già avviate per violazioni degli obblighi di cui al presente decreto, l'imposizione degli obblighi di cui al capo IV e l'esercizio dei poteri di cui al capo V.

Art. 6.

Soggetti essenziali e soggetti importanti

1. Ai fini del presente decreto, sono considerati soggetti essenziali:

a) i soggetti di cui all'allegato I che superano i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE;

b) indipendentemente dalle loro dimensioni, i soggetti identificati come soggetti critici ai sensi del decreto legislativo che recepisce la direttiva (UE) 2022/2557;

c) i fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui all'articolo 3, comma 5, lettera *b)*, che si considerano medie imprese ai sensi dell'articolo 2 dell'allegato alla raccomandazione 2003/361/CE;

d) indipendentemente dalle loro dimensioni, i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio di cui all'articolo 3, comma 5, lettere *c)* e *d)*;

e) indipendentemente dalle loro dimensioni, le pubbliche amministrazioni centrali di cui all'allegato III, comma 1, lettera *a)*.

2. Fermo restando quanto previsto dal comma 1, l'Autorità nazionale competente NIS individua, secondo le modalità di cui all'articolo 40, comma 5, i soggetti di cui all'articolo 3, commi 6, 8, 9 e 10, che, indipendentemente dalle loro dimensioni, sono considerati essenziali.

3. Ai fini del presente decreto, sono considerati soggetti importanti i soggetti di cui all'articolo 3 che non sono considerati essenziali ai sensi dei commi 1 e 2 del presente articolo.

Art. 7.

Identificazione ed elencazione dei soggetti essenziali e dei soggetti importanti

1. Dal 1° gennaio al 28 febbraio di ogni anno successivo alla data di entrata in vigore del presente decreto, i soggetti di cui all'articolo 3, si registrano o aggiornano la propria registrazione sulla piattaforma digitale resa disponibile dall'Autorità nazionale competente NIS ai fini dello svolgimento delle funzioni attribuite all'Agenzia per la cybersicurezza nazionale anche ai sensi del presente decreto. A tal fine, tali soggetti forniscono o aggiornano almeno le informazioni seguenti:

a) la ragione sociale;

b) l'indirizzo e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono;

c) la designazione di un punto di contatto, indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono;

d) ove applicabile, i pertinenti settori, sottosettori e tipologie di soggetto di cui agli allegati I, II, III e IV;

2. Entro il 31 marzo di ogni anno successivo alla data di entrata in vigore del presente decreto, l'Autorità nazionale competente NIS, redige, secondo le modalità di cui all'articolo 40, comma 5, l'elenco dei soggetti essenziali e dei soggetti importanti, sulla base delle registrazioni di cui al comma 1 e delle decisioni adottate ai sensi degli articoli 3, 4, e 6.

3. Tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS comunica ai soggetti registrati di cui al comma 2:

a) l'inserimento nell'elenco dei soggetti essenziali o importanti;

b) la permanenza nell'elenco dei soggetti essenziali o importanti;

c) l'espunzione dall'elenco dei soggetti.

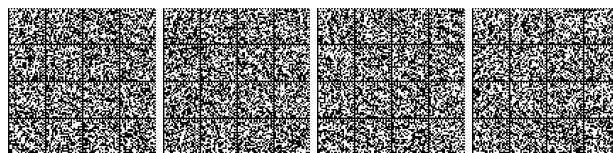
4. Dal 15 aprile al 31 maggio di ogni anno successivo alla data di entrata in vigore del presente decreto, tramite la piattaforma digitale di cui al comma 1, i soggetti che hanno ricevuto la comunicazione di cui al comma 3, lettere *a)* e *b)*, forniscono o aggiornano almeno le informazioni seguenti:

a) lo spazio di indirizzamento IP pubblico e i nomi di dominio in uso o nella disponibilità del soggetto;

b) ove applicabile, l'elenco degli Stati membri in cui forniscono servizi che rientrano nell'ambito di applicazione del presente decreto;

c) i responsabili di cui all'articolo 38, comma 5, indicando il ruolo presso il soggetto e i loro recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono;

d) un sostituto del punto di contatto di cui al comma 1, lettera *c)*, indicando il ruolo presso il soggetto e i recapiti aggiornati, compresi gli indirizzi e-mail e i numeri di telefono.

5. I fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione

dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, i fornitori di motori di ricerca online e i fornitori di piattaforme di social network, forniscono all'Autorità nazionale competente NIS, secondo le modalità di cui al comma 4, anche:

a) l'indirizzo della sede principale e delle altre sedi del soggetto nell'Unione europea;

b) se non è stabilito nell'Unione europea, l'indirizzo della sede del suo rappresentante ai sensi dell'articolo 5, comma 3, unitamente ai dati di contatto aggiornati, compresi gli indirizzi e-mail e i numeri di telefono.

6. L'Autorità nazionale competente NIS stabilisce, secondo le modalità di cui all'articolo 40, comma 5, i termini, le modalità e i procedimenti di utilizzo e accesso alla piattaforma digitale di cui al comma 1, indicando altresì eventuali ulteriori informazioni che i soggetti devono fornire ai sensi dei commi 1 e 4, nonché i termini, le modalità e i procedimenti di designazione dei rappresentanti di cui all'articolo 5, comma 3.

7. I soggetti che hanno ricevuto la comunicazione di cui al comma 3, lettere *a)* e *b)*, notificano all'Autorità nazionale competente NIS, tramite la piattaforma digitale di cui al comma 1, qualsiasi modifica delle informazioni trasmesse ai sensi del presente articolo tempestivamente e, in ogni caso, entro quattordici giorni dalla data della modifica.

Art. 8.

Protezione dei dati personali

1. L'Agenzia per la cybersicurezza nazionale, le Autorità di settore NIS e i soggetti di cui all'articolo 3 trattano i dati personali nella misura necessaria ai fini del presente decreto e conformemente al decreto legislativo 30 giugno 2003, n. 196 e al regolamento (UE) 2016/679.

2. Il trattamento dei dati personali ai sensi del presente decreto da parte dei fornitori di reti pubbliche di comunicazione elettronica o dei fornitori di servizi di comunicazione elettronica accessibili al pubblico viene effettuato in conformità della legislazione dell'Unione europea in materia di protezione dei dati e della legislazione dell'Unione europea in materia di tutela della vita privata, ai sensi della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002.

Capo II

QUADRO NAZIONALE DI SICUREZZA INFORMATICA

Art. 9.

Strategia nazionale di cybersicurezza

1. La Strategia nazionale di cybersicurezza individua gli obiettivi strategici e le risorse necessarie per conseguirli, nonché adeguate misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cybersicurezza.

2. La Strategia nazionale di cybersicurezza comprende almeno:

a) gli obiettivi e le priorità, che riguardano in particolare i settori di cui agli allegati I, II, III e IV;

b) un quadro di governance per la realizzazione degli obiettivi e delle priorità di cui alla lettera *a)*, comprendente le misure strategiche di cui al comma 3;

c) un quadro di governance che chiarisca i ruoli e le responsabilità dei pertinenti portatori di interessi a livello nazionale, a sostegno della cooperazione e del coordinamento a livello nazionale tra le Autorità di settore NIS, l'Agenzia per la cybersicurezza nazionale, in qualità di Autorità nazionale competente NIS, di Punto di contatto unico NIS e di CSIRT Italia, nonché il coordinamento e la cooperazione tra tali organismi e le altre autorità competenti ai sensi degli atti giuridici settoriali dell'Unione europea;

d) un meccanismo per individuare le risorse e una valutazione dei rischi a livello nazionale;

e) l'individuazione delle misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato;

f) un elenco delle diverse autorità e dei diversi portatori di interessi coinvolti nell'attuazione della strategia nazionale per la cybersicurezza;

g) un quadro strategico per il coordinamento rafforzato tra le autorità competenti ai sensi del presente decreto e le autorità competenti di cui al decreto legislativo di recepimento della direttiva (UE) 2022/2557 ai fini della condivisione delle informazioni sui rischi, le minacce e gli incidenti sia informatici che non informatici e dello svolgimento di compiti di vigilanza, in modo adeguato;

h) un piano, comprendente le misure necessarie, per aumentare il livello generale di consapevolezza dei cittadini in materia di sicurezza informatica.

3. Nell'ambito della strategia nazionale per la cybersicurezza, sono previste, inoltre, le seguenti misure strategiche:

a) la sicurezza informatica nella catena di approvvigionamento dei prodotti e dei servizi TIC utilizzati dai soggetti per la fornitura dei loro servizi;

b) l'inclusione e la definizione di requisiti concernenti la sicurezza informatica per i prodotti e i servizi TIC negli appalti pubblici, compresi i requisiti relativi alla certificazione della cybersicurezza, alla cifratura e all'utilizzo di prodotti di sicurezza informatica open source;

c) la gestione delle vulnerabilità, ivi comprese la promozione e l'agevolazione della divulgazione coordinata delle vulnerabilità di cui all'articolo 16;

d) il sostegno della disponibilità generale, dell'integrità e della riservatezza del nucleo pubblico della rete internet aperta, compresa, se del caso, la sicurezza informatica dei cavi di comunicazione sottomarini;

e) la promozione dello sviluppo e dell'integrazione di tecnologie avanzate rilevanti, volte ad attuare misure all'avanguardia nella gestione dei rischi per la sicurezza informatica;

f) la promozione e lo sviluppo di attività di istruzione, formazione e sensibilizzazione, di competenze e di iniziative di ricerca e sviluppo in materia di sicurezza informatica, nonché orientamenti sulle buone pratiche e sui controlli concernenti l'igiene informatica, destinati ai cittadini, ai portatori di interessi e ai soggetti essenziali e importanti;

g) il sostegno agli istituti accademici e di ricerca volto a sviluppare, rafforzare e promuovere la diffusione di strumenti di sicurezza informatica e di infrastrutture di rete sicure;

h) la messa a punto di procedure pertinenti e strumenti adeguati di condivisione delle informazioni per sostenere la condivisione volontaria di informazioni sulla sicurezza informatica tra soggetti, nel rispetto del diritto dell'Unione europea;

i) il rafforzamento dei valori di riferimento relativi alla resilienza e all'igiene informatica delle piccole e medie imprese, in particolare quelle escluse dall'ambito di applicazione del presente decreto, fornendo orientamenti e sostegno facilmente accessibili per le loro esigenze specifiche;

l) la promozione di una protezione informatica attiva.

4. Ferme restando le funzioni del Presidente del Consiglio dei ministri di cui all'articolo 2, commi 1 e 2, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, l'Agenzia per la cybersicurezza nazionale provvede ai sensi dell'articolo 7 del citato decreto-legge n. 82 del 2021, sentite le amministrazioni componenti il Nucleo per la cybersicurezza, alla periodica valutazione della Strategia nazionale di cybersicurezza, nonché al suo aggiornamento ove necessario e comunque almeno ogni cinque anni sulla base di indicatori chiave di prestazione, proponendone l'adozione al Presidente del Consiglio dei ministri con le modalità di all'articolo 2, comma 1, lettera *b)*, del medesimo decreto-legge.

Art. 10.

Autorità nazionale competente e Punto di contatto unico

1. L'Agenzia per la cybersicurezza nazionale è l'Autorità nazionale competente NIS di cui all'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555 e pertanto:

a) sovrintende all'implementazione e all'attuazione del presente decreto;

b) predispone i provvedimenti necessari a dare attuazione al presente decreto;

c) svolge le funzioni e le attività di regolamentazione di cui al presente decreto, anche adottando linee guida, raccomandazioni e orientamenti non vincolanti;

d) individua i soggetti essenziali e i soggetti importanti ai sensi degli articoli 3 e 6, nonché redige l'elenco di cui all'articolo 7, comma 2;

e) partecipa al Gruppo di cooperazione NIS, nonché ai consessi e alle iniziative promosse a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555;

f) definisce gli obblighi di cui all'articolo 7, comma 6, e al capo IV;

g) svolge le attività ed esercita i poteri di cui al capo V.

2. L'Agenzia per la cybersicurezza nazionale è il Punto di contatto unico NIS di cui all'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555, svolgendo una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità nazionali con le autorità pertinenti degli altri Stati membri, la Commissione e l'ENISA.

3. Ai fini dell'attuazione del presente articolo è autorizzata la spesa pari a euro 2.000.000 annui a decorrere dall'anno 2025 a cui si provvede ai sensi dell'articolo 44.

Art. 11.

Autorità di settore NIS

1. Al fine di assicurare l'efficace attuazione del presente decreto a livello settoriale, sono individuate le Autorità di settore NIS che supportano l'Autorità nazionale competente NIS e collaborano con essa, secondo le modalità di cui all'articolo 40, comma 2, lettera *c)*.

2. Sono designate quali Autorità di settore NIS:

a) la Presidenza del Consiglio dei ministri per:

1) il settore gestione dei servizi TIC, di cui al numero 9 dell'allegato I, in collaborazione con l'Agenzia per la cybersicurezza nazionale;

2) il settore dello spazio, di cui al numero 10 dell'allegato I;

3) il settore delle pubbliche amministrazioni, di cui all'articolo 3, commi 6 e 7;

4) le società in house e le società partecipate o a controllo pubblico, di cui al numero 4 dell'allegato IV;

b) il Ministero dell'economia e delle finanze, per i settori bancario e delle infrastrutture dei mercati finanziari, di cui ai numeri 3 e 4 dell'allegato I, sentite le autorità di vigilanza di settore, Banca d'Italia e Consob;

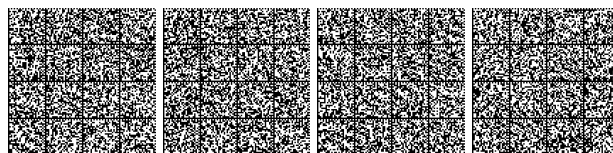
c) il Ministero delle imprese e del made in Italy per:

1) il settore delle infrastrutture digitali, di cui al numero 8 dell'allegato I;

2) il settore dei servizi postali e di corriere, di cui al numero 1 dell'allegato II;

3) il settore della fabbricazione, produzione e distribuzione di sostanze chimiche, di cui al numero 3 dell'allegato II, sentito il Ministero della salute;

4) i sottosettori della fabbricazione di computer e prodotti di elettronica e ottica, della fabbricazione di apparecchiature elettriche e della fabbricazione di macchinari e apparecchiature non classificati altrove (n.c.a.), di cui, rispettivamente, alle lettere *b)*, *c)* e *d)* del settore fabbricazione, di cui al numero 5 dell'allegato II;

5) i sottosettori della fabbricazione di autoveicoli, rimorchi e semirimorchi, e della fabbricazione di altri mezzi di trasporto, di cui, rispettivamente, alle lettere *e)* e *f)* del settore fabbricazione, di cui al numero 5 dell'allegato II, sentito il Ministero delle infrastrutture e dei trasporti;

6) i fornitori di servizi digitali, di cui al numero 6 dell'allegato II;

d) il Ministero dell'agricoltura, della sovranità alimentare e delle foreste per il settore produzione, trasformazione e distribuzione di alimenti, di cui al numero 4 dell'allegato II;

e) il Ministero dell'ambiente e della sicurezza energetica per:

1) il settore energia, di cui al numero 1 dell'allegato I;

2) il settore fornitura e distribuzione di acqua potabile di cui al numero 6 dell'allegato I;

3) il settore acque reflue, di cui al numero 7 dell'allegato I;

4) il settore gestione dei rifiuti, di cui al numero 2 dell'allegato II;

f) il Ministero delle infrastrutture e dei trasporti per:

1) il settore trasporti, di cui al numero 2 dell'allegato I;

2) i soggetti che forniscono servizi di trasporto pubblico locale di cui al numero 1 dell'allegato IV;

g) il Ministero dell'università e della ricerca per il settore ricerca di cui al numero 7 dell'allegato II e per gli istituti di istruzione che svolgono attività di ricerca di cui al numero 2 dell'allegato IV, anche in accordo con le altre amministrazioni vigilanti;

h) il Ministero della cultura per i soggetti che svolgono attività di interesse culturale di cui al numero 3 dell'allegato IV;

i) il Ministero della salute per:

1) il settore sanitario, di cui al numero 5 dell'allegato I;

2) il sottosettore fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro, di cui alla lettera *a)* del settore fabbricazione, di cui al numero 5 dell'allegato II.

3. Le Amministrazioni di cui al comma 2, per i rispettivi settori e sottosettori di competenza, sono altresì designate Autorità di settore per i soggetti di cui all'articolo 3, commi 9 e 10.

4. Le Autorità di settore NIS, per i rispettivi settori e sottosettori di competenza ai fini di cui al comma 1, procedono, in particolare:

a) alla verifica dell'elenco dei soggetti di cui all'articolo 7, comma 2;

b) al supporto nell'individuazione dei soggetti essenziali e dei soggetti importanti ai sensi degli articoli 3 e 6, in particolare identificando i soggetti essenziali e i soggetti importanti di cui ai commi 8, 9 e 10 dell'articolo 3;

c) all'individuazione dei soggetti a cui si applicano le deroghe di cui all'articolo 3, comma 4;

d) al supporto per le funzioni e per le attività di regolamentazione di cui al presente decreto secondo le modalità di cui all'articolo 40;

e) all'elaborazione dei contributi per la relazione annuale di cui all'articolo 12, comma 5, lettera *c)*;

f) all'istituzione e al coordinamento dei tavoli settoriali, al fine di contribuire all'efficace e coerente attuazione settoriale del presente decreto nonché al relativo monitoraggio. Per la partecipazione ai tavoli settoriali non sono previsti gettoni di presenza, compensi, rimborsi di spese o emolumenti comunque denominati;

g) alla partecipazione alle attività settoriali del Gruppo di Cooperazione NIS nonché dei consessi e delle iniziative a livello di Unione europea relativi all'attuazione della direttiva (UE) 2022/2555.

5. Con accordo sancito entro il 30 ottobre 2024 in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono definite modalità di collaborazione tra le Autorità di settore e le regioni e le province autonome di Trento e di Bolzano interessate, quando il soggetto critico ha carattere regionale ovvero opera esclusivamente sul territorio di una regione o di una provincia autonoma nei settori di cui al comma 2, lettere *a)*, numeri 3 e 4, *d)*, *e)*, *f)*, *h)* e *i)*, numero 1.

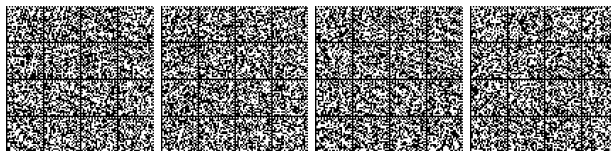
6. Per l'esercizio delle competenze attribuite dal presente decreto, ciascuna autorità di settore, ad eccezione di quella indicata al comma 2, lettera *b)*, è autorizzata a reclutare, con contratto di lavoro subordinato a tempo indeterminato, n. 2 unità di personale non dirigenziale, appartenente all'area funzionari del vigente contratto collettivo nazionale - Comparto funzioni centrali, o categorie equivalenti, mediante procedure di passaggio diretto di personale tra amministrazioni pubbliche ai sensi dell'articolo 30 del decreto legislativo 30 marzo 2001, n. 165, scorrimento di vigenti graduatorie di concorsi pubblici o avvio di nuove procedure concorsuali pubbliche, nonché ad avvalersi di personale non dirigenziale posto in posizione di comando, ai sensi dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127, di aspettativa, distacco o fuori ruolo ovvero altro analogo istituto previsto dai rispettivi ordinamenti, ad esclusione del personale docente, educativo, amministrativo, tecnico e ausiliario delle istituzioni scolastiche. All'atto del collocamento fuori ruolo è reso indisponibile, nella dotazione organica dell'amministrazione di provenienza, per tutta la durata del collocamento fuori ruolo, un numero di posti equivalente dal punto di vista finanziario.

7. Per l'attuazione del comma 6 del presente articolo è autorizzata la spesa di 409.424 euro per l'anno 2024 e di euro 925.695 annui a decorrere dall'anno 2025, a cui si provvede ai sensi dell'articolo 44.

Art. 12.

Tavolo per l'attuazione della disciplina NIS

1. Presso l'Agenzia per la cybersicurezza nazionale è costituito, in via permanente, il Tavolo per l'attuazione della disciplina NIS, per assicurare l'implementazione e attuazione del presente decreto.

2. Il Tavolo per l'attuazione della disciplina NIS è presieduto dal direttore generale dell'Agenzia per la cybersicurezza nazionale, o da un suo delegato, ed è composto da un rappresentante di ogni Autorità di settore NIS di cui all'articolo 11 e da due rappresentanti designati da regioni e province autonome in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano.

3. I componenti del Tavolo per l'attuazione della disciplina NIS possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati dalle previsioni di cui al presente decreto.

4. Il Tavolo per l'attuazione della disciplina NIS è convocato su indicazione del presidente o su richiesta di almeno tre componenti e si riunisce almeno una volta per trimestre.

5. Per le finalità di cui al comma 1, il Tavolo per l'attuazione della disciplina NIS:

a) supporta l'Autorità nazionale competente NIS nello svolgimento delle funzioni relative all'implementazione e all'attuazione del presente decreto, con particolare riferimento a quanto previsto dall'articolo 10, comma 1, lettere da *a)* a *f)*;

b) formula proposte e pareri per l'adozione di iniziative, linee guida o atti di indirizzo ai fini dell'efficace attuazione del presente decreto;

c) predispone una relazione annuale sull'attuazione del presente decreto.

6. Con le modalità di cui all'articolo 40, comma 5, possono essere dettate ulteriori disposizioni per l'organizzazione e per il funzionamento del Tavolo. Per la partecipazione al Tavolo per l'attuazione della disciplina NIS non sono previsti gettoni di presenza, compensi, rimborsi di spese o altri emolumenti, comunque denominati.

Art. 13.

Quadro nazionale di gestione delle crisi informatiche

1. L'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e il Ministero della difesa sono individuati quali Autorità nazionali di gestione delle crisi informatiche, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera *g)*.

2. Le Autorità nazionali di gestione delle crisi informatiche individuano le capacità, le risorse e le procedure che possono essere impiegate in caso di crisi ai fini del presente decreto.

3. Entro dodici mesi dalla data di entrata in vigore del presente decreto, con uno o più decreti del Presidente del Consiglio dei ministri, su proposta dell'Agenzia per la cybersicurezza nazionale e del Ministero della difesa, ciascuno per gli ambiti di competenza di cui all'articolo 2, comma 1, lettera *g)*, previo parere del Comitato interministeriale per la sicurezza della Repubblica nella composizione di cui all'articolo 10 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, è definito il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala. Il piano di cui al primo periodo è aggiornato periodicamente e, comunque, ogni tre anni.

4. Il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala stabilisce gli obiettivi e le modalità di gestione dei medesimi. In tale piano sono definiti, in particolare:

a) gli obiettivi delle misure e delle attività nazionali di preparazione;

b) i compiti e le responsabilità delle Autorità nazionali di gestione delle crisi informatiche;

c) le procedure di gestione delle crisi informatiche, tra cui la loro integrazione nel quadro nazionale per la gestione delle crisi che coinvolgono aspetti di cybersicurezza di cui all'articolo 10 del decreto-legge n. 82 del 2021, e i canali di scambio di informazioni;

d) le misure nazionali di preparazione, comprese le esercitazioni e le attività di formazione;

e) i pertinenti portatori di interessi del settore pubblico e privato e le infrastrutture coinvolte;

f) le procedure nazionali e gli accordi tra gli organismi e le autorità nazionali pertinenti al fine di garantire il sostegno e la partecipazione effettivi dell'Italia alla gestione coordinata degli incidenti e delle crisi informatiche su vasta scala a livello dell'Unione europea.

5. I decreti del Presidente del Consiglio dei ministri di cui al presente articolo sono esclusi dall'accesso e non sono soggetti a pubblicazione.

6. Ai fini dell'attuazione del comma 1 del presente articolo è autorizzata la spesa pari a euro 1.000.000 annui a decorrere dall'anno 2025, a cui si provvede ai sensi dell'articolo 44.

Art. 14.

Cooperazione tra Autorità nazionali

1. Sono assicurate la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS con l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (Autorità di contrasto), con il Garante per la protezione dei dati personali quale autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679, con l'Ente nazionale per l'aviazione civile (ENAC) quale autorità nazionale ai sensi dei regolamenti (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, e (UE) 2018/1139, del Parlamento europeo e del Consiglio, del 4 luglio 2018, con l'Agenzia per l'Italia digitale (AgID) quale organismo di vigilanza ai sensi del regolamento (UE) n. 910/2014, con l'Autorità per le garanzie nelle comunicazioni quale autorità nazionale di regolamentazione ai sensi della direttiva (UE) 2018/1972, con il Ministero della difesa, quale responsabile in materia di difesa dello Stato, nonché con altre autorità nazionali competenti anche ai sensi di altri atti giuridici settoriali dell'Unione europea, ivi incluso lo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

2. Ai fini della cooperazione e della collaborazione di cui al comma 1:

a) l'Autorità nazionale competente NIS coopera con il Garante per la protezione dei dati personali, ai sensi

dell'articolo 7, comma 5, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, nei casi di incidenti che comportano violazioni di dati personali, ai sensi del regolamento (UE) 2016/679, senza pregiudicare la competenza e i compiti di controllo di cui al citato regolamento;

b) qualora l'Autorità nazionale competente NIS, in sede di vigilanza o di esecuzione, venga a conoscenza del fatto che la violazione degli obblighi di cui all'articolo 24 da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali, quale definita all'articolo 4, punto 12), del regolamento (UE) 2016/679, che deve essere notificata ai sensi dell'articolo 33 del medesimo regolamento, ne informa senza indebito ritardo il Garante per la protezione dei dati personali ai sensi dell'articolo 55 o 56 di tale regolamento;

c) qualora il Garante per la protezione dei dati personali o le autorità di controllo di altri Stati membri di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria ai sensi dell'articolo 58, paragrafo 2, lettera *i)*, del medesimo regolamento, l'Autorità nazionale competente NIS non procede all'irrogazione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 38 per una violazione di cui alla lettera *b)* del presente comma, imputabile al medesimo comportamento. L'Autorità nazionale competente NIS può tuttavia esercitare i poteri di esecuzione di cui all'articolo 37;

d) con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della difesa, sentita l'Agenzia per la cybersicurezza nazionale, è definito, nell'ambito dell'elenco di cui all'articolo 7, comma 2, l'elenco dei soggetti che impattano sulla efficienza dello Strumento militare e sulla tutela della difesa e sicurezza militare dello Stato, su cui l'Autorità nazionale competente NIS comunica tempestivamente al Ministero della difesa gli incidenti di cui all'articolo 25, nonché, con le modalità previste nel decreto di cui alla presente lettera, le ulteriori informazioni di sicurezza cibernetica.

3. La cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS con le autorità nazionali competenti di cui al regolamento (UE) 2022/2554 è assicurata con gli strumenti di cui al medesimo regolamento (UE) 2022/2554 e alla disciplina nazionale di attuazione, in relazione, tra l'altro, allo scambio periodico di informazioni pertinenti, anche per quanto riguarda gli incidenti e le minacce informatiche rilevanti.

4. L'Autorità nazionale competente NIS coopera con le pertinenti autorità nazionali competenti degli altri Stati membri, di cui al regolamento (UE) 2022/2554. In particolare, l'Autorità nazionale competente NIS informa il forum di sorveglianza istituito ai sensi dell'articolo 32, paragrafo 1, del regolamento (UE) 2022/2554 quando esercita i propri poteri di vigilanza ed esecuzione finalizzati a garantire il rispetto degli obblighi previsti dal presente decreto da parte di un soggetto essenziale o importante designato come fornitore terzo critico di servizi di TIC ai sensi dell'articolo 31 del regolamento (UE) 2022/2554.

5. È assicurata la cooperazione e la collaborazione reciproca dell'Autorità nazionale competente NIS e del Punto di contatto unico NIS, secondo le modalità di cui all'articolo 40, comma 3, con le autorità nazionali competenti e il punto di contatto unico ai sensi della direttiva (UE) 2022/2557, anche attraverso lo scambio periodico di informazioni riguardo all'identificazione di soggetti critici, sui rischi, sulle minacce e sugli incidenti sia informatici che non informatici che interessano i soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557, e sulle misure adottate in risposta a tali rischi, minacce e incidenti.

6. Ai fini della cooperazione e della collaborazione di cui al comma 5:

a) il punto di contatto unico e le autorità competenti di cui al decreto legislativo di recepimento della direttiva (UE) 2022/2557 comunicano tempestivamente all'Autorità nazionale competente NIS i soggetti identificati come soggetti critici ai sensi del medesimo decreto legislativo e i successivi aggiornamenti;

b) le autorità nazionali competenti ai sensi del decreto legislativo di recepimento della direttiva (UE) 2022/2557 possono chiedere all'Autorità nazionale competente NIS di svolgere le attività ed esercitare i poteri di cui al capo V in relazione a un soggetto che è stato individuato come soggetto critico ai sensi del citato decreto legislativo.

Art. 15.

Gruppo nazionale di risposta agli incidenti di sicurezza informatica - CSIRT Italia

1. Il CSIRT Italia, fermo restando quanto previsto dal decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109:

a) è l'organo preposto alle funzioni di gestione degli incidenti di sicurezza informatica per i settori, i sottosettori e le tipologie di soggetti di cui agli allegati I, II, III e IV, conformemente a modalità e procedure definite dal CSIRT stesso;

b) dispone di un'infrastruttura di informazione e comunicazione appropriata, sicura e resiliente a livello nazionale attraverso la quale scambiare informazioni con i soggetti essenziali o importanti e con gli altri portatori di interesse pertinenti;

c) coopera e, se opportuno, scambia informazioni pertinenti conformemente all'articolo 17 con comunità settoriali o intersettoriali di soggetti essenziali e di soggetti importanti;

d) partecipa alla revisione tra pari di cui all'articolo 21;

e) garantisce la collaborazione effettiva, efficiente e sicura, nella Rete di CSIRT nazionali di cui all'articolo 20;

f) ai sensi dell'articolo 7, comma 1, lettera *s)*, del decreto-legge n. 82 del 2021, può stabilire relazioni di cooperazione con gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi. Nell'ambito di tali relazioni di cooperazione, facilita uno scambio di informazioni efficace, efficiente e sicuro con tali CSIRT nazionali, o strutture nazionali equivalenti di Paesi terzi, utilizzando i pertinenti protocolli di condivisione delle informazioni, ivi inclusi quelli adottati e sviluppati dal-

le principali comunità nazionali, europee e internazionali del settore. Il CSIRT Italia può scambiare informazioni pertinenti con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi o con organismi equivalenti di Paesi terzi, compresi dati personali ai sensi della normativa nazionale vigente e del diritto dell'Unione europea in materia di protezione dei dati personali;

g) ai sensi dell'articolo 7, comma 1, lettera *s)*, del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, può cooperare con Gruppi nazionali di risposta agli incidenti di sicurezza informatica di Paesi terzi o con organismi equivalenti di Paesi terzi, in particolare al fine di fornire loro assistenza in materia di sicurezza informatica.

2. Il CSIRT Italia:

a) è dotato di un alto livello di disponibilità dei propri canali di comunicazione evitando singoli punti di malfunzionamento e dispone di mezzi che gli permettono di essere contattato e di contattare i soggetti essenziali o importanti e altri CSIRT nazionali in qualsiasi momento. Il CSIRT Italia indica chiaramente i canali di comunicazione e li rende noti ai soggetti essenziali e importanti e agli altri CSIRT nazionali;

b) dispone di locali e sistemi informativi di supporto ubicati in siti sicuri;

c) utilizza un sistema adeguato di gestione e inoltro delle richieste, in particolare per facilitare i trasferimenti in maniera efficace ed efficiente;

d) garantisce la riservatezza e l'affidabilità delle proprie attività;

e) è dotato di sistemi ridondanti e spazi di lavoro di backup al fine di garantire la continuità dei propri servizi;

f) partecipa, se del caso, a reti di cooperazione internazionale.

3. Il CSIRT Italia svolge i seguenti compiti:

a) monitora e analizza le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale e, su richiesta, fornisce assistenza ai soggetti essenziali e ai soggetti importanti interessati per quanto riguarda il monitoraggio in tempo reale o prossimo al reale dei loro sistemi informativi e di rete, secondo un ordine di priorità delle attività definito dal medesimo CSIRT Italia, onde evitare oneri sproporzionati o eccessivi;

b) emette preallarmi, allerte e bollettini e divulga informazioni ai soggetti essenziali e ai soggetti importanti interessati, nonché alle autorità nazionali competenti e agli altri pertinenti portatori di interessi, in merito a minacce informatiche, vulnerabilità e incidenti, se possibile in tempo prossimo al reale;

c) fornisce una risposta agli incidenti e assistenza ai soggetti essenziali e ai soggetti importanti interessati, ove possibile;

d) raccoglie e analizza dati forensi e fornisce un'analisi dinamica dei rischi e degli incidenti, nonché una consapevolezza situazionale riguardo alla sicurezza informatica;

e) effettua, su richiesta di un soggetto essenziale o importante, secondo modalità e procedure definite, una scansione proattiva dei sistemi informativi e di rete del soggetto interessato per rilevare le vulnerabilità con potenziale impatto significativo;

f) partecipa alla Rete di CSIRT nazionali di cui all'articolo 20 e fornisce assistenza reciproca secondo le proprie capacità e competenze agli altri membri della Rete di CSIRT nazionali su loro richiesta;

g) agisce in qualità di coordinatore ai fini del processo di divulgazione coordinata delle vulnerabilità di cui all'articolo 16;

h) contribuisce allo sviluppo di strumenti sicuri per la condivisione delle informazioni di cui al comma 1, lettera *b)*;

i) può effettuare, secondo modalità e procedure definite, una scansione proattiva e non intrusiva dei sistemi informativi e di rete accessibili al pubblico di soggetti essenziali e di soggetti importanti. Tale scansione è effettuata per individuare sistemi informativi e di rete vulnerabili o configurati in modo non sicuro e per informare i soggetti interessati. Tale scansione non ha alcun impatto negativo sul funzionamento dei servizi dei soggetti.

4. Il CSIRT Italia applica un approccio basato sul rischio per stabilire l'ordine di priorità nello svolgimento dei compiti di cui al comma 3.

5. In caso di eventi malevoli per la sicurezza informatica, le strutture pubbliche con funzione di *computer emergency response team* (CERT) collaborano con il CSIRT Italia, anche ai fini di un più efficace coordinamento della risposta agli incidenti.

6. Il CSIRT Italia instaura rapporti di cooperazione con i pertinenti portatori di interesse nazionali del settore privato al fine di perseguire gli obiettivi del presente decreto in relazione alle proprie competenze.

7. Al fine di agevolare la cooperazione di cui al comma 5, il CSIRT Italia promuove l'adozione e l'uso di pratiche, sistemi di classificazione e tassonomie standardizzati o comuni per quanto riguarda:

a) le procedure di gestione degli incidenti;

b) la divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 16.

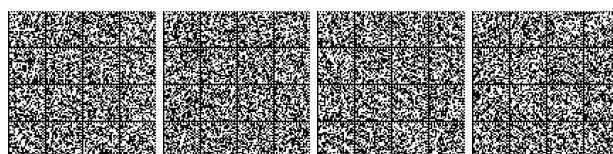
8. Ai fini dell'attuazione del presente articolo è autorizzata la spesa pari a euro 2.000.000 annui a decorrere dall'anno 2025, a cui si provvede ai sensi dell'articolo 44.

Art. 16.

Divulgazione coordinata delle vulnerabilità

1. Il CSIRT Italia è designato coordinatore ai fini della divulgazione coordinata delle vulnerabilità ai sensi dell'articolo 12 della direttiva (UE) 2022/2555 e agisce da intermediario di fiducia agevolando, se necessario, l'interazione tra la persona fisica o giuridica che segnala la vulnerabilità e il fabbricante o fornitore di servizi TIC o prodotti TIC potenzialmente vulnerabili, su richiesta di una delle parti.

2. I compiti del CSIRT Italia in veste di coordinatore comprendono:

a) l'individuazione e il contatto dei soggetti interessati;

b) l'assistenza alle persone fisiche o giuridiche che segnalano una vulnerabilità;

c) la negoziazione dei tempi di divulgazione e la gestione delle vulnerabilità che interessano più soggetti.

3. Le persone fisiche o giuridiche possono segnalare in forma anonima, qualora lo richiedano, una vulnerabilità al CSIRT Italia. Quest'ultimo, in veste di coordinatore, garantisce lo svolgimento di diligenti azioni per dare seguito alla segnalazione di vulnerabilità e assicura l'anonimato della persona fisica o giuridica segnalante. Se la vulnerabilità segnalata è suscettibile di avere un impatto significativo su soggetti in più di uno Stato membro, il CSIRT Italia coopera, ove opportuno, con altri CSIRT designati in qualità di coordinatori nell'ambito della Rete di CSIRT nazionali di cui all'articolo 20.

4. L'Autorità nazionale competente NIS adotta, secondo le modalità di cui all'articolo 40, comma 5, una politica nazionale di divulgazione coordinata delle vulnerabilità in linea con le previsioni del presente decreto e tenuto conto degli orientamenti non vincolanti del Gruppo di cooperazione NIS. L'Agenzia per la cybersicurezza nazionale implementa mezzi tecnici per agevolare l'attuazione della politica nazionale di divulgazione coordinata delle vulnerabilità.

Art. 17.

Accordi di condivisione delle informazioni sulla sicurezza informatica

1. I soggetti che rientrano nell'ambito di applicazione del presente decreto e laddove opportuno anche ulteriori soggetti, possono scambiarsi, su base volontaria, pertinenti informazioni sulla sicurezza informatica, comprese informazioni relative a minacce informatiche, quasi-incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di sicurezza informatica e raccomandazioni concernenti la configurazione degli strumenti di sicurezza informatica per individuare le minacce informatiche, se tale condivisione di informazioni:

a) mira a prevenire o rilevare gli incidenti, a recuperare dagli stessi o a mitigarne l'impatto;

b) aumenta il livello di sicurezza informatica, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di mitigazione o fasi di risposta e recupero, oppure promuovendo la ricerca collaborativa sulle minacce informatiche tra soggetti pubblici e privati.

2. Lo scambio di informazioni di cui al comma 1 avviene nell'ambito di comunità di soggetti essenziali e di soggetti importanti e, se opportuno, nell'ambito dei loro fornitori o fornitori di servizi. Tale scambio è attuato mediante accordi di condivisione delle informazioni sulla sicurezza informatica che tengono conto della natura potenzialmente sensibile delle informazioni condivise.

3. L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, ove possibile, tenuto conto degli orientamenti e delle migliori pratiche non vincolanti elaborati dall'ENISA, favorisce la conclusione degli accordi di condivisione delle informazioni sulla sicurezza informatica di cui al comma 2 e può specificare gli elementi operativi, compreso l'uso di piattaforme TIC dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni. Nello stabilire i dettagli relativi alla partecipazione delle autorità pubbliche a tali accordi, l'Autorità nazionale competente NIS può imporre condizioni, secondo le modalità di cui all'articolo 40, comma 5, alinea, per le informazioni messe a disposizione dalle autorità competenti e dal CSIRT Italia. L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, supporta i soggetti essenziali e i soggetti importanti per l'applicazione di tali accordi conformemente alle loro misure strategiche di cui all'articolo 9, comma 3, lettera *h)*.

4. I soggetti essenziali e i soggetti importanti notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica di cui al comma 2 al momento della conclusione di tali accordi o, ove applicabile, del loro ritiro da tali accordi, una volta che questo è divenuto effettivo.

5. È assicurato l'accesso degli Organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge n. 124 del 2007 alle informazioni riguardanti l'elenco dei soggetti essenziali e dei soggetti importanti, tramite la piattaforma digitale di cui all'articolo 7, le notifiche di cui agli articoli 25 e 26, le vulnerabilità rilevate nell'applicazione del presente decreto, e le ulteriori informazioni rispetto a quelle di cui al presente comma che dovessero essere ritenute utili, relative alle attività di cui al presente decreto, previe intese tra i predetti Organismi e l'Agenzia per la cybersicurezza nazionale.

Capo III

COOPERAZIONE A LIVELLO DELL'UNIONE EUROPEA E INTERNAZIONALE

Art. 18.

Gruppo di cooperazione NIS

1. L'Autorità nazionale competente NIS partecipa al Gruppo di cooperazione NIS.

2. Le Autorità di settore NIS partecipano, su richiesta dell'Autorità nazionale competente NIS, alle iniziative del Gruppo di cooperazione NIS relative al proprio settore di interesse.

3. Ai fini dei commi 1 e 2, l'Autorità nazionale competente NIS, supportata dalle Autorità di settore NIS interessate, provvede a:

a) tenere conto degli orientamenti non vincolanti del Gruppo di cooperazione NIS in merito al recepimento e all'attuazione della direttiva (UE) 2022/2555;

b) tenere conto degli orientamenti non vincolanti del Gruppo di cooperazione NIS in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 16;

c) scambiare migliori prassi e informazioni relative all'attuazione della direttiva (UE) 2022/2555, anche per quanto riguarda minacce informatiche, incidenti, vulnerabilità, quasi-incidenti, iniziative di sensibilizzazione, attività di formazione, esercitazioni e competenze, sviluppo di capacità, specifiche tecniche anche adottate da un organismo di normazione riconosciuto di cui al regolamento (UE) 1025/2012, nonché all'identificazione dei soggetti essenziali e dei soggetti importanti ai sensi del presente decreto;

d) effettuare scambi di opinioni per quanto riguarda l'attuazione degli atti giuridici settoriali dell'Unione europea che contengono disposizioni in materia di sicurezza informatica;

e) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 21;

f) richiedere, se del caso, una discussione sulle relazioni sulle revisioni tra pari di cui all'articolo 21 che coinvolgono l'Autorità nazionale competente NIS e l'elaborazione di conclusioni e di raccomandazioni a riguardo;

g) discutere casi di assistenza reciproca, ivi incluse le esperienze e i risultati delle azioni di vigilanza comuni transfrontaliere di cui all'articolo 39;

h) su richiesta di uno o più Stati membri, discutere le richieste specifiche di assistenza reciproca di cui all'articolo 39;

i) richiedere, se opportuno, la discussione di richieste specifiche di assistenza reciproca di cui all'articolo 39 che coinvolgono l'Autorità nazionale competente NIS;

l) scambiare opinioni su misure per mitigare la ricorrenza di incidenti e crisi di sicurezza informatica su vasta scala sulla base degli insegnamenti tratti da EU–CyCLONe e dalla Rete di CSIRT nazionali;

m) partecipare, ove necessario, ai programmi di sviluppo delle capacità, anche prevedendo lo scambio di personale tre le Autorità nazionali e quelle di altri Stati membri;

n) discutere le attività intraprese per quanto riguarda le esercitazioni in materia di sicurezza informatica, comprese le attività svolte dall'ENISA;

o) partecipare alle riunioni congiunte con il gruppo per la resilienza dei soggetti critici istituito ai sensi della direttiva (UE) 2022/2557, volte a promuovere e ad agevolare la cooperazione strategica e lo scambio di informazioni nell'attuazione della direttiva medesima e della direttiva (UE) 2022/2555.

4. Inoltre, ai fini dei commi 1 e 2, l'Autorità nazionale competente NIS, supportata dalle Autorità di settore NIS interessate, contribuisce:

a) alla definizione degli orientamenti non vincolanti per le autorità competenti in merito al recepimento e all'attuazione della direttiva (UE) 2022/2555;

b) alla definizione degli orientamenti non vincolanti del Gruppo di cooperazione NIS in merito allo sviluppo e all'attuazione di politiche in materia di divulgazione coordinata delle vulnerabilità di cui all'articolo 16;

c) alla definizione di pareri non vincolanti e alla cooperazione con la Commissione europea per quanto riguarda le nuove iniziative strategiche in materia di sicurezza informatica e la coerenza dei requisiti settoriali di informatica;

d) alla definizione di pareri non vincolanti e alla cooperazione con la Commissione europea per quanto riguarda i progetti di atti delegati o di esecuzione adottati ai sensi della direttiva (UE) 2022/2555;

e) allo scambio delle migliori prassi e di informazioni con le istituzioni, gli organismi, gli uffici e le agenzie pertinenti dell'Unione europea;

f) se del caso, all'elaborazione di conclusioni e di raccomandazioni circa le relazioni sulle revisioni tra pari di cui all'articolo 21;

g) all'elaborazione delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche conformemente all'articolo 22, paragrafo 1, della direttiva (UE) 2022/2555;

h) alla definizione degli orientamenti strategici per EU–CyCLONe e per la Rete di CSIRT nazionali su specifiche questioni emergenti;

i) al rafforzamento delle capacità di sicurezza informatica a livello dell'Unione europea;

l) all'organizzazione di riunioni congiunte periodiche con i pertinenti portatori di interessi del settore privato dell'Unione europea per discutere le attività svolte dal Gruppo di cooperazione NIS e raccogliere contributi sulle sfide strategiche emergenti;

m) alla definizione della metodologia e degli aspetti organizzativi delle revisioni tra pari di cui all'articolo 21 nonché della metodologia di autovalutazione per gli Stati membri e all'elaborazione dei codici di condotta su cui si basano i metodi di lavoro degli esperti di sicurezza informatica designati di cui al medesimo articolo;

n) all'elaborazione delle relazioni, ai fini del riesame di cui all'articolo 40 della direttiva (UE) 2022/2555, sull'esperienza acquisita a livello strategico e dalle revisioni tra pari sull'attuazione della direttiva stessa;

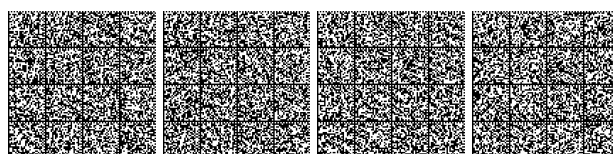
o) alla discussione e allo svolgimento periodico di valutazione dello stato di avanzamento delle minacce o degli incidenti informatici, ivi inclusi i ransomware;

p) alla collaborazione con l'ENISA e con la Commissione europea per la pubblicazione della relazione biennale sullo stato della sicurezza informatica nell'Unione europea di cui all'articolo 18, paragrafo 1, della direttiva (UE) 2022/2555;

q) alla collaborazione con l'ENISA, con la Commissione europea e con la Rete di CSIRT nazionali, per la definizione della metodologia di cui all'articolo 18, paragrafo 3, della direttiva (UE) 2022/2555, per l'elaborazione della relazione biennale sullo stato della sicurezza informatica nell'Unione europea.

Art. 19.

Rete delle organizzazioni di collegamento per le crisi informatiche - EU-CyCLONe

1. L'Autorità nazionale di gestione delle crisi informatiche partecipa alla Rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe).

2. Ai fini del comma 1, l'Autorità nazionale di gestione delle crisi informatiche contribuisce a:

a) aumentare il livello di preparazione per la gestione di incidenti e crisi informatiche su vasta scala;

b) sviluppare una conoscenza situazionale condivisa in merito agli incidenti e alle crisi informatiche su vasta scala;

c) valutare le conseguenze e l'impatto degli incidenti e delle crisi informatiche su vasta scala e proporre possibili misure di attenuazione;

d) coordinare la gestione degli incidenti e delle crisi informatiche su vasta scala e sostenere il processo decisionale a livello politico in merito a tali incidenti e crisi;

e) discutere, su richiesta di uno Stato membro interessato, i piani nazionali di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 9, paragrafo 4, della direttiva (UE) 2022/2555;

f) supportare la collaborazione con il Gruppo di cooperazione NIS al fine di aggiornarlo in merito alla gestione degli incidenti e delle crisi informatiche su vasta scala, nonché in merito alle tendenze, concentrandosi in particolare sul relativo impatto sui soggetti essenziali e sui soggetti importanti;

g) cooperare con la Rete di CSIRT nazionali;

h) elaborare la relazione al Parlamento europeo e al Consiglio sulla valutazione del lavoro della Rete di cui all'articolo 16, paragrafo 7, della direttiva (UE) 2022/2555.

3. L'Autorità nazionale di gestione delle crisi informatiche, ai sensi del comma 2, lettera *e)*, può richiedere di discutere il piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3.

Art. 20.

Rete di CSIRT nazionali

1. Il CSIRT Italia partecipa alla Rete di CSIRT nazionali.

2. Il CSIRT Italia, ai fini del comma 1, contribuisce a:

a) scambiare informazioni per quanto riguarda le capacità dei CSIRT nazionali;

b) agevolare, ove possibile, la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT nazionali;

c) scambiare, su richiesta di un CSIRT nazionale di un altro Stato membro potenzialmente interessato da un incidente, informazioni relative a tale incidente, alle minacce informatiche, ai rischi e alle vulnerabilità associate;

d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di sicurezza informatica;

e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni;

f) su richiesta di un membro della Rete di CSIRT nazionali potenzialmente interessato da un incidente, scambiare e discutere informazioni non sensibili sul piano commerciale connesse a tale incidente, ai rischi e alle vulnerabilità associati, ad eccezione dei casi in cui lo scambio di informazioni potrebbe compromettere l'indagine sull'incidente;

g) su richiesta di un membro della Rete di CSIRT nazionali, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro;

h) fornire assistenza ai CSIRT nazionali di altri Stati membri nel far fronte a incidenti che interessano due o più Stati membri;

i) cooperare e scambiare migliori pratiche con i CSIRT nazionali designati dagli altri Stati membri in qualità di coordinatori ai sensi dell'articolo 12 della direttiva (UE) 2022/2555, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro;

l) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a:

1) categorie di minacce informatiche e incidenti;

2) preallarmi;

3) assistenza reciproca;

4) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri;

5) contributi al piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3, su richiesta di uno Stato membro;

m) su richiesta di un membro della Rete di CSIRT nazionali, discutere le capacità e lo stato di preparazione del CSIRT nazionale richiedente;

n) cooperare e scambiare informazioni con i centri operativi di sicurezza informatica regionali e a livello dell'Unione europea, al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche a livello dell'Unione europea;

o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 21;

p) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi-incidenti, le minacce informatiche, i rischi e le vulnerabilità;

q) informare il Gruppo di cooperazione NIS sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera *i)* e, se necessario, chiedere orientamenti non vincolanti in merito;

r) fare il punto sui risultati delle esercitazioni di sicurezza informatica, comprese quelle organizzate dall'ENISA;

s) fornire orientamenti non vincolanti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa.

Art. 21.

Procedura di revisione tra pari

1. L'Autorità nazionale competente NIS può partecipare alla procedura di revisione tra pari, di cui all'articolo 19 della direttiva (UE) 2022/2555, nel quadro della

metodologia di cui all'articolo 18, comma 4, lettera *m)*, del presente decreto:

a) richiedendo l'esecuzione di una revisione tra pari in relazione all'attuazione della direttiva (UE) 2022/2555 a livello nazionale;

b) indicando uno o più rappresentanti dell'Agenzia per la cybersicurezza nazionale o delle Autorità di settore NIS quali esperti di sicurezza informatica, di cui all'articolo 19, paragrafo 2, della direttiva (UE) 2022/2555, per eseguire revisioni tra pari presso altri Stati membri, su richiesta di questi ultimi, nel rispetto dei codici di condotta di cui all'articolo 18, comma 4, lettera *m)*, del presente decreto. Eventuali rischi di conflitto di interessi riguardanti gli esperti di sicurezza informatica designati sono condivisi con gli altri Stati membri, il Gruppo di cooperazione NIS, la Commissione europea e l'ENISA prima dell'inizio della revisione tra pari.

2. Ai fini di cui al comma 1, lettera *a)*, l'Autorità nazionale competente NIS, con le modalità di cui all'articolo 40, comma 5, alinea:

a) provvede a identificare almeno un aspetto da sottoporre alla revisione tra pari tra i seguenti:

1) il livello di attuazione degli obblighi in materia di misure di gestione del rischio e di notifica degli incidenti di cui agli articoli 24 e 25;

2) il livello delle capacità, comprese le risorse finanziarie, tecniche e umane disponibili, e l'efficacia dello svolgimento dei compiti dell'Autorità medesima;

3) le capacità operative del CSIRT Italia;

4) lo stato di attuazione dell'assistenza reciproca di cui all'articolo 39;

5) lo stato di attuazione degli accordi per la condivisione delle informazioni in materia di sicurezza informatica di cui all'articolo 17;

6) questioni specifiche di natura transfrontaliera o intersettoriale;

b) notifica, prima dell'inizio della revisione tra pari, agli Stati membri partecipanti, l'ambito di applicazione della medesima, comprese le questioni specifiche individuate;

c) effettua, se del caso, un'autovalutazione degli aspetti oggetto della revisione;

d) seleziona, tra gli esperti di sicurezza informatica indicati dagli altri Stati membri partecipanti, gli esperti idonei da designare. Qualora l'Autorità nazionale competente NIS si opponga alla designazione di uno o più esperti indicati, comunica allo Stato membro indicante i motivi debitamente giustificati;

e) fornisce, se del caso, l'autovalutazione di cui alla lettera *c)* agli esperti designati di cui alla lettera *d)*;

f) fornisce agli esperti designati di cui alla lettera *d)* le informazioni necessarie per la valutazione, anche con visite in loco fisiche o virtuali, nonché scambi di informazioni a distanza;

g) formula, se del caso, osservazioni sulla relazione elaborata dagli esperti designati di cui alla lettera *d)*;

h) può decidere di rendere pubblica la relazione elaborata dagli esperti designati di cui alla lettera *d)*, alla quale sono allegate, in tutto o in parte, le osservazioni di cui alla lettera *g)*.

3. Ai fini di cui al comma 1, lettera *b)*, gli esperti di sicurezza informatica indicati dall'Autorità nazionale competente NIS:

a) non divulgano a terzi le eventuali informazioni sensibili o riservate ottenute nel corso delle revisioni tra pari a cui partecipano;

b) partecipano alle attività necessarie allo svolgimento delle revisioni tra pari tramite visite in loco fisiche o virtuali e scambi di informazioni a distanza;

c) contribuiscono all'elaborazione delle relazioni sui risultati e sulle conclusioni delle revisioni tra pari.

4. La condivisione delle informazioni ai sensi del presente articolo è effettuata nel rispetto della legislazione nazionale o dell'Unione europea in materia di tutela delle informazioni protette da classifica di segretezza e di salvaguardia delle funzioni essenziali dello Stato, ivi inclusa la sicurezza nazionale.

Art. 22.

Comunicazioni all'Unione europea

1. Successivamente alla data di entrata in vigore del presente decreto, la Presidenza del Consiglio dei ministri notifica tempestivamente alla Commissione europea la conferma dell'Agenzia per la cybersicurezza nazionale quale Autorità nazionale competente NIS e quale Punto di contatto unico NIS, nonché la designazione dell'Agenzia per la cybersicurezza nazionale, con funzioni di coordinatore ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2555, e del Ministero della difesa, quali Autorità nazionali di gestione delle crisi informatiche, e i relativi ambiti di competenza come indicati all'articolo 2, comma 1, lettera *g)*. Successivamente, ogni ulteriore modifica a tali designazioni o compiti è notificata, senza ingiustificato ritardo, alla Commissione europea. Alle designazioni sono assicurate idonee forme di pubblicità.

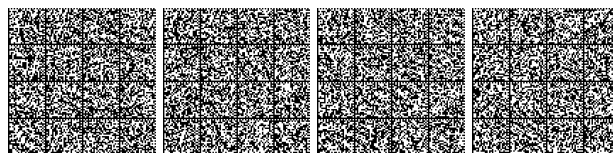
2. L'Autorità nazionale competente NIS:

a) trasmette alla Commissione europea la Strategia nazionale di cybersicurezza di cui all'articolo 9 entro tre mesi dalla sua adozione o dal suo aggiornamento. Possono essere esclusi dalla trasmissione gli elementi della strategia riguardanti la sicurezza nazionale e quelli ulteriori rispetto alle previsioni del presente decreto;

b) comunica entro il 17 gennaio 2025 alla Commissione europea le misure sanzionatorie e le disposizioni che stabiliscono sanzioni nei confronti dei soggetti essenziali e dei soggetti importanti di cui al presente decreto. Successivamente, è comunicata ogni ulteriore modifica a tali misure e disposizioni;

c) comunica entro il 17 aprile 2025 e, successivamente, ogni due anni:

1) alla Commissione europea e al Gruppo di cooperazione NIS, il numero dei soggetti essenziali e dei soggetti importanti inclusi nell'elenco di cui all'articolo 7, comma 2, per ciascun settore e sottosettore di cui agli allegati I, II e III;

2) alla Commissione europea informazioni pertinenti sul numero di soggetti essenziali e di soggetti importanti individuati ai sensi dell'articolo 3, comma 9, lettere da *b)* a *e)*, sui settori e i sottosettori di cui agli allegati I, II e III ai quali appartengono, sul tipo di servizio

che forniscono e sui criteri di cui all'articolo 3, comma 9, lettere da *b)* a *e)*, per i quali sono stati individuati;

d) su richiesta della Commissione europea, può notificare a quest'ultima, in tutto o in parte, le denominazioni dei soggetti essenziali e dei soggetti importanti di cui alla lettera *c)*, numero 2);

e) comunica all'ENISA, senza ingiustificato ritardo e comunque entro quattordici giorni dalla loro ricezione, le informazioni di cui all'articolo 7, comma 1, lettere *a)*, *b)* e *d)*, comma 4, lettera *b)*, e comma 5, lettere *a)* e *b)*, fornite dai soggetti di cui a quest'ultimo comma, per l'inserimento nel registro di cui all'articolo 27 della direttiva (UE) 2022/2555. L'Autorità nazionale competente NIS può richiedere all'ENISA l'accesso a tale registro, assicurando la tutela della riservatezza delle informazioni ivi contenute.

3. Il Punto di contatto unico NIS:

a) successivamente alla data di entrata in vigore del presente decreto, comunica alla Commissione europea, senza ingiustificato ritardo, la designazione dell'Agenzia per la cybersicurezza nazionale quale CSIRT nazionale, denominato CSIRT Italia, e quale coordinatore conformemente all'articolo 16, i rispettivi compiti in relazione ai soggetti essenziali e ai soggetti importanti e qualsiasi ulteriore modifica dei medesimi;

b) trasmette all'ENISA, ogni trimestre a partire dal 1° gennaio 2026, una relazione di sintesi che comprende dati anonimizzati e aggregati sugli incidenti significativi, sugli incidenti, sulle minacce informatiche e sui quasi-incidenti notificati ai sensi degli articoli 25 e 26;

c) trasmette, successivamente alla data di entrata in vigore del presente decreto, senza ingiustificato ritardo, le notifiche di incidente con effetti transfrontalieri di cui agli articoli 25 e 26 ai punti di contatto unici degli altri Stati membri interessati e all'ENISA.

4. L'Autorità nazionale di gestione delle crisi informatiche comunica entro tre mesi dall'adozione o dall'aggiornamento del piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3, alla Commissione europea e alla Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) le informazioni pertinenti relative ai requisiti di cui all'articolo 13, comma 4, in merito al proprio piano nazionale di risposta agli incidenti e alle crisi informatiche su vasta scala, fatto salvo quanto previsto dall'articolo 4, commi 1, 7 e 8.

Capo IV

OBBLIGHI IN MATERIA DI GESTIONE DEL RISCHIO PER LA SICUREZZA INFORMATICA E DI NOTIFICA DI INCIDENTE

Art. 23.

Organi di amministrazione e direttivi

1. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

a) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;

b) sovrintendono all'implementazione degli obblighi di cui al presente capo e di cui all'articolo 7;

c) sono responsabili delle violazioni di cui al presente decreto.

2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

a) sono tenuti a seguire una formazione in materia di sicurezza informatica;

b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera *a)* ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

3. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli articoli 25 e 26.

Art. 24.

Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica

1. I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tali misure:

a) assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;

b) sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

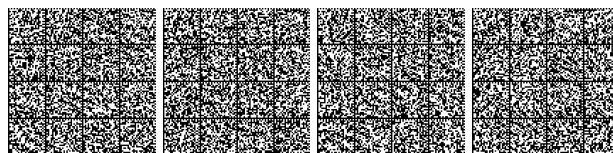
a) politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;

b) gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;

c) continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;

d) sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;

e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;

f) politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;

g) pratiche di igiene di base e di formazione in materia di sicurezza informatica;

h) politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;

i) sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;

l) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

3. Nel valutare quali misure di cui al comma 2, lettera *d)*, siano adeguate, i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

4. Qualora un soggetto rilevi di non essere conforme alle misure di cui al comma 2, esso adotta, senza indebito ritardo, tutte le misure appropriate e proporzionate correttive necessarie.

Art. 25.

Obblighi in materia di notifica di incidente

1. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

2. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale impatto transfrontaliero dell'incidente.

3. La notifica non espone il soggetto che la effettua a una maggiore responsabilità rispetto a quella derivante dall'incidente.

4. Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

5. Ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia:

a) senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b) senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera *a)* e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera *b)*, che comprenda:

1) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;

2) il tipo di minaccia o la causa originale (*root cause*) che ha probabilmente innescato l'incidente;

3) le misure di attenuazione adottate e in corso;

4) ove noto, l'impatto transfrontaliero dell'incidente;

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera *d)*, una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

6. In deroga a quanto previsto dal comma 5, lettera *b)*, un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, provvede alla notifica di cui alla medesima lettera, senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo.

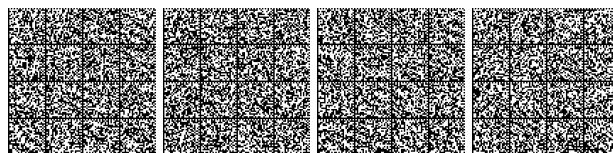
7. Fermo restando quanto previsto dall'articolo 15, comma 4, senza ingiustificato ritardo e ove possibile entro 24 ore dal ricevimento della pre-notifica di cui al comma 5, lettera *a)*, il CSIRT Italia fornisce una risposta al soggetto notificante, comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione. Su richiesta del soggetto notificante, il CSIRT Italia fornisce ulteriore supporto tecnico.

8. Qualora si sospetti che l'incidente significativo abbia carattere criminale, il CSIRT Italia fornisce al soggetto notificante anche orientamenti sulla segnalazione dell'incidente significativo, all'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 (Autorità di contrasto).

9. Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i soggetti essenziali e i soggetti importanti comunicano, senza ingiustificato ritardo, ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

10. I soggetti essenziali e i soggetti importanti, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, comunicano senza ingiustificato ritardo, ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, i soggetti essenziali e i soggetti importanti comunicano ai medesimi destinatari anche la natura di tale minaccia informatica significativa.

11. L'Agenzia per la cybersicurezza nazionale, nello svolgimento delle funzioni di Autorità nazionale competente NIS e di CSIRT Italia, anche sentendo, se del caso, le autorità competenti e gli CSIRT nazionali degli altri Stati membri interessati, può informare il pubblico riguar-

do all'incidente significativo per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso, o qualora ritenga che la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico.

12. L'Agenzia per la cybersicurezza nazionale adotta mezzi tecnici e relative procedure per semplificare le notifiche di cui al presente articolo e le notifiche volontarie di cui all'articolo 26, informando i soggetti essenziali e i soggetti importanti.

Art. 26.

Notifica volontaria di informazioni pertinenti

1. In aggiunta all'obbligo di notifica di incidente di cui all'articolo 25, possono essere trasmesse, su base volontaria, notifiche al CSIRT Italia da parte dei:

a) soggetti essenziali e soggetti importanti, per quanto riguarda gli incidenti diversi da quelli di cui all'articolo 25, comma 1, le minacce informatiche e i quasi-incidenti;

b) soggetti diversi da quelli di cui alla lettera *a)*, indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione del presente decreto, per quanto riguarda gli incidenti che hanno un impatto significativo sulla fornitura dei loro servizi, le minacce informatiche e i quasi-incidenti.

2. Il CSIRT Italia:

a) tratta le notifiche volontarie applicando la procedura di cui all'articolo 25;

b) tratta le notifiche di incidente di cui all'articolo 25 prioritariamente rispetto alle notifiche volontarie;

c) tratta le notifiche volontarie soltanto qualora ciò non costituisca un onere sproporzionato o eccessivo.

3. Fatte salve le esigenze di indagine, accertamento e perseguimento di reati, la notifica volontaria di cui al comma 1 non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

Art. 27.

Uso di schemi di certificazione della cybersicurezza

1. Al fine di dimostrare il rispetto di determinati obblighi di cui all'articolo 24, l'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 5, può imporre ai soggetti essenziali e ai soggetti importanti di utilizzare categorie di prodotti TIC, servizi TIC e processi TIC, di cui, rispettivamente, all'articolo 2, comma 1, lettere *ff)*, *gg)* e *hh)*, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito dei sistemi europei di certificazione della cybersicurezza di cui all'articolo 49 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019. L'Autorità nazionale competente NIS promuove, altresì, l'utilizzo di servizi fiduciari qualificati da parte dei soggetti essenziali e dei soggetti importanti.

2. Nelle more dell'adozione di pertinenti sistemi europei di certificazione della cybersicurezza di cui all'articolo 49 del regolamento (UE) 2019/881, l'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 5, può imporre ai soggetti essenziali e ai soggetti importanti di utilizzare categorie di prodotti TIC, servizi TIC e processi TIC, sviluppati dal soggetto essenziale o importante o acquistati da terze parti, che siano certificati nell'ambito di schemi di certificazione riconosciuti a livello nazionale o europeo.

Art. 28.

Specifiche tecniche

1. Per favorire l'attuazione efficace e armonizzata dell'articolo 24, commi 1 e 2, l'Autorità nazionale competente NIS, senza imposizioni o discriminazioni a favore dell'uso di un particolare tipo di tecnologia, promuove l'uso di specifiche tecniche europee e internazionali, anche adottate da un organismo di normazione riconosciuto di cui al regolamento (UE) 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, relative alla sicurezza dei sistemi informativi e di rete.

2. Ai fini del comma 1, l'Autorità nazionale competente NIS tiene conto delle linee guida e degli orientamenti non vincolanti elaborati dall'ENISA ai sensi dell'articolo 25, paragrafo 2, della direttiva (UE) 2022/2555 e può redigere e aggiornare periodicamente un elenco delle categorie di tecnologie più idonee ad assicurare l'effettiva attivazione delle misure di gestione dei rischi per la sicurezza informatica.

3. L'elenco di cui al comma 2 non ha carattere vincolante o esaustivo ed è pubblicato sul sito dell'Agenzia per la cybersicurezza nazionale al fine di fornire un orientamento sulle specifiche tecniche, di cui al comma 1, e sulle norme di settore nazionali ed europee applicabili alle tipologie di soggetti di cui agli allegati I, II, III e IV al presente decreto.

Art. 29.

Banca dei dati di registrazione dei nomi di dominio

1. Per contribuire alla sicurezza, alla stabilità e alla resilienza dei sistemi di nomi di dominio, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio raccolgono e mantengono dati di registrazione dei nomi di dominio accurati e completi in un'apposita banca dati con la dovuta diligenza, conformemente al diritto dell'Unione europea in materia di protezione dei dati personali.

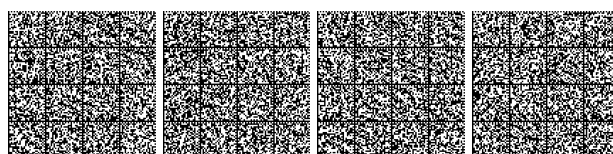
2. Ai fini del comma 1, la banca dei dati di registrazione dei nomi di dominio contiene le informazioni necessarie per identificare e contattare i titolari dei nomi di dominio e i punti di contatto che amministrano i nomi di dominio presenti, registrati o censiti nel registro dei nomi di dominio di primo livello (*top level domain - TLD)*. Tali informazioni includono, almeno:

a) il nome di dominio;

b) la data di registrazione;

c) il nome, l'indirizzo e-mail di contatto e il numero di telefono del soggetto che procede alla registrazione;

d) l'indirizzo e-mail di contatto e il numero di telefono del punto di contatto che amministra il nome di dominio qualora siano diversi da quelli del soggetto che procede alla registrazione.

3. I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio predispongono e rendono pubbliche politiche e

procedure, incluse le procedure di verifica, al fine di garantire che le banche dati di cui al comma 1 contengano informazioni accurate e complete.

4. I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio per i domini di primo livello rendono pubblicamente disponibili, senza ingiustificato ritardo dopo la registrazione di un nome di dominio, i dati di registrazione dei nomi di dominio che non sono dati personali.

5. I gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio, su richiesta motivata dei soggetti legittimati, forniscono l'accesso a specifici dati di registrazione dei nomi di dominio, nel rispetto del diritto dell'Unione europea in materia di protezione dei dati. I soggetti che gestiscono i registri dei nomi di dominio di primo livello e i soggetti che forniscono servizi di registrazione dei nomi di dominio rispondono senza ingiustificato ritardo e, comunque, entro 72 ore dalla ricezione della richiesta di accesso. Tale risposta reca gli specifici dati di registrazione dei nomi di dominio richiesti, ovvero le motivazioni per cui la richiesta non è stata ritenuta legittima o debitamente motivata. Le politiche e le procedure relative alla divulgazione di tali dati hanno evidenza pubblica.

6. Ai fini del comma 5, l'Agenzia per la cybersicurezza nazionale può richiedere l'accesso ai dati di registrazione dei nomi di dominio e può stipulare appositi protocolli con i gestori di registri dei nomi di dominio di primo livello e i fornitori di registrazione dei nomi di dominio.

7. Al fine di evitare una duplicazione della raccolta di dati di registrazione dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello e i fornitori di servizi di registrazione dei nomi di dominio individuano modalità e procedure di collaborazione per la raccolta e il mantenimento dei dati di cui al comma 1.

Art. 30.

Elencazione, caratterizzazione e categorizzazione delle attività e dei servizi

1. Ai fini di cui all'articolo 24, comma 1, dal 1° maggio al 30 giugno di ogni anno a partire dalla ricezione della prima comunicazione di cui all'articolo 7, comma 3, lettera *a)*, i soggetti essenziali e i soggetti importanti comunicano e aggiornano, tramite la piattaforma digitale di cui all'articolo 7, comma 1, un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza.

2. L'Autorità nazionale competente NIS stabilisce, secondo le modalità di cui all'articolo 40, comma 5, anche tenuto conto di quanto previsto dall'articolo 25, comma 1, le categorie di rilevanza nonché il processo, le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi di cui al presente articolo.

3. Entro novanta giorni dalla comunicazione tramite la piattaforma digitale di cui al comma 1, l'Autorità nazionale competente NIS fornisce riscontro ai soggetti essenziali e ai soggetti importanti circa la conformità di quanto comunicato rispetto alle modalità e ai criteri di cui al comma 2. Il predetto termine può essere prorogato dall'Autorità nazionale competente NIS, per una sola volta e fino ad un massimo di ulteriori sessanta giorni, qualora sia necessario svolgere approfondimenti. Ove si renda necessario richiedere integrazioni e informazioni aggiuntive ai soggetti essenziali o importanti, i termini di cui al presente comma sono interrotti sino alla data di ricevimento delle predette integrazioni e informazioni, che sono rese entro il termine di trenta giorni dalla richiesta.

4. In assenza del riscontro di cui al comma 3 da parte dall'Autorità nazionale competente NIS entro i termini di cui al medesimo comma, la conformità di cui al comma 3 si intende convalidata.

5. Ai fini del presente articolo, l'Autorità nazionale competente NIS può avvalersi dei tavoli settoriali di cui all'articolo 11, comma 4, lettera *f)*.

Art. 31.

Proporzionalità e gradualità degli obblighi

1. Ai fini di cui agli articoli 23, 24, 25, 27, 28 e 29 l'Autorità nazionale competente NIS stabilisce obblighi proporzionati tenuto debitamente conto del grado di esposizione dei soggetti ai rischi, delle dimensioni dei soggetti e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

2. L'Autorità nazionale competente NIS stabilisce termini, modalità, specifiche e tempi graduali di implementazione degli obblighi di cui al comma 1, secondo le modalità di cui all'articolo 40, comma 5, anche differenziandoli in relazione:

a) alle categorie di rilevanza di cui all'articolo 30, comma 2, delle attività e dei servizi che i sistemi informativi e di rete supportano, svolgono o erogano;

b) al settore, al sottosettore e alla tipologia di soggetto, tenendo conto del grado di maturità iniziale nell'ambito della sicurezza informatica;

c) all'individuazione del soggetto quale essenziale o importante.

3. L'Autorità nazionale competente NIS individua, se del caso, le fattispecie che determinano la sospensione dei termini di cui al comma 2.

4. L'Autorità nazionale competente NIS può emanare linee guida vincolanti per l'attuazione degli obblighi di cui al presente capo.

5. L'Autorità nazionale competente NIS può emanare raccomandazioni per supportare i soggetti nell'implementazione degli obblighi di cui al presente capo.

6. Ai fini del presente articolo, l'Autorità nazionale competente NIS può avvalersi dei tavoli settoriali di cui all'articolo 11, comma 4, lettera *f)*.

7. Le comunicazioni e le interazioni dei soggetti con l'Autorità nazionale competente NIS avvengono, in via prioritaria, per mezzo della piattaforma digitale di cui all'articolo 7, comma 1.

Art. 32.

Previsioni settoriali specifiche

1. Fermo restando quanto previsto dagli articoli 23, 24, 25, 27, 28 e 29, tenuto conto degli impatti sociali e economici di un incidente significativo nella catena di approvvigionamento del settore della pubblica amministrazione, l'Autorità nazionale competente NIS, secondo le modali-

tà di cui all'articolo 40, comma 5, può imporre specifici obblighi proporzionati e graduali ai soggetti essenziali e ai soggetti importanti che forniscono servizi, anche digitali, alla pubblica amministrazione.

2. L'Autorità nazionale competente NIS, secondo le modalità di cui all'articolo 40, comma 5, può individuare gli obblighi di cui al presente capo che non si applicano:

a) alle amministrazioni pubbliche di cui all'allegato III, lettere *c)* e *d)*;

b) ai soggetti di cui all'articolo 3, comma 8, comma 9, lettera *f)*, e comma 10.

3. Gli obblighi di cui agli articoli 24 e 25 non si applicano ai soggetti che erogano esclusivamente servizi di registrazione dei nomi di dominio. Tali soggetti assicurano un livello di sicurezza informatica coerente con gli obblighi di cui agli articoli 24 e 25.

4. La designazione o la mancata designazione del rappresentante di cui all'articolo 5, comma 3, non pregiudica l'applicabilità degli obblighi di cui al presente capo.

Art. 33.

Coordinamento con la disciplina del perimetro di sicurezza nazionale cibernetica

1. Ai fini dell'articolo 4:

a) gli obblighi di gestione del rischio per la sicurezza informatica e di notifica di incidente previsti dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, sono considerati almeno equivalenti a quelli previsti dal presente decreto;

b) alle reti, ai sistemi informativi e ai servizi informatici inseriti nell'elenco di cui all'articolo 1, comma 2, lettera *b)*, del decreto-legge n. 105 del 2019, non si applicano le disposizioni di cui al presente decreto. Restano fermi gli obblighi del presente decreto per i sistemi informativi e di rete diversi da quelli di cui al primo periodo;

c) i soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019, non sono sottoposti agli obblighi di notifica di cui all'articolo 25 del presente decreto per gli incidenti riconducibili a una notifica effettuata ai sensi dell'articolo 1, comma 3, del medesimo decreto-legge;

d) le informazioni attinenti ai soggetti di cui all'articolo 1, comma 2-*bis*, del decreto-legge n. 105 del 2019, ovvero trasmesse da questi ultimi all'Agenzia per la cybersicurezza nazionale ai sensi del presente decreto, possono essere escluse dagli obblighi di comunicazione di cui all'articolo 22.

Capo V

MONITORAGGIO, VIGILANZA ED ESECUZIONE

Art. 34.

Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione

1. L'Autorità nazionale competente NIS monitora e valuta il rispetto da parte dei soggetti essenziali e dei soggetti importanti degli obblighi previsti dall'articolo 7 e dal capo IV, nonché i relativi effetti sulla sicurezza dei sistemi informativi e di rete, svolgendo attività di vigilanza attraverso:

a) il monitoraggio, l'analisi e il supporto ai soggetti essenziali e ai soggetti importanti;

b) la verifica e le ispezioni;

c) l'adozione di misure di esecuzione;

d) l'irrogazione di sanzioni amministrative pecuniarie e accessorie.

2. L'Autorità nazionale competente NIS può conferire priorità alle attività di cui al presente capo adottando un approccio basato sul rischio.

3. L'Autorità nazionale competente NIS provvede affinché le attività di vigilanza imposte ai soggetti per quanto riguarda gli obblighi di cui al presente decreto siano effettive, proporzionate e dissuasive, tenuto conto di ciascuna fattispecie e dei criteri di cui all'articolo 31.

4. L'Autorità nazionale competente NIS vigila sul rispetto, da parte degli enti della pubblica amministrazione, del presente decreto, con indipendenza operativa rispetto agli enti della pubblica amministrazione sottoposti a vigilanza.

5. L'Autorità nazionale competente NIS espone nei particolari la motivazione per l'adozione dei provvedimenti per lo svolgimento delle attività e l'esercizio dei poteri di cui al presente capo.

6. Le attività e i poteri di cui al presente capo sono rispettivamente svolte ed esercitati rispettando i diritti della difesa nonché tenendo conto delle circostanze di ciascuna fattispecie e almeno dei seguenti elementi:

a) la gravità della violazione e l'importanza delle disposizioni violate, considerando gravi in particolare:

1) le violazioni ripetute;

2) la mancata notifica di incidenti significativi o il mancato rimedio a tali incidenti;

3) il mancato rimedio alle carenze a seguito di istruzioni vincolanti emesse dall'Autorità nazionale competente NIS;

4) l'ostacolo alle attività di vigilanza di cui al presente capo;

5) la fornitura di informazioni false o gravemente inesatte relative agli obblighi di cui al presente decreto;

b) la durata della violazione;

c) eventuali precedenti violazioni pertinenti commesse dal soggetto interessato;

d) qualsiasi danno materiale o immateriale causato, incluse le perdite finanziarie o economiche, gli effetti sugli altri servizi e il numero di utenti interessati;

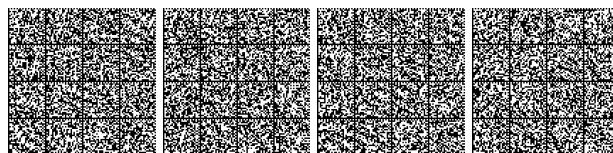
e) un'eventuale condotta intenzionale o negligenza da parte dell'autore della violazione;

f) qualsiasi misura adottata dal soggetto per prevenire o attenuare il danno materiale o immateriale;

g) qualsiasi adesione a codici di condotta o meccanismi di certificazione approvati;

h) il livello di collaborazione delle persone fisiche o giuridiche ritenute responsabili con l'Autorità nazionale competente NIS.

7. Gli audit sulla sicurezza, periodici e mirati, nonché le scansioni di sicurezza di cui agli articoli 35 e 37, sono svolti da organismi indipendenti e si basano su valutazioni del rischio effettuate dall'Autorità nazionale com-

petente NIS o dal soggetto sottoposto ad audit o su altre informazioni disponibili in relazione ai rischi. L'Autorità nazionale competente NIS può richiedere, anche solo in parte, di acquisire gli esiti di tali audit sulla sicurezza e di tali scansioni di sicurezza. I costi di tali audit sulla sicurezza e di tali scansioni di sicurezza sono a carico del soggetto sottoposto ad audit, salvo in casi debitamente giustificati in cui l'Autorità nazionale competente NIS decida altrimenti, in linea con il piano di risposta agli incidenti e alle crisi informatiche su vasta scala di cui all'articolo 13, comma 3.

8. La designazione o la mancata designazione del rappresentante di cui all'articolo 5, comma 3, non pregiudica lo svolgimento delle attività e l'esercizio dei poteri di cui al presente capo.

9. Le comunicazioni e le interazioni dei soggetti con l'Autorità nazionale competente NIS avvengono, in via prioritaria, per mezzo della piattaforma digitale di cui all'articolo 7, comma 1.

10. Con decreto del Presidente del Consiglio dei ministri, da adottare secondo le modalità di cui all'articolo 40, comma 1, sono stabiliti i criteri, le procedure e le modalità per lo svolgimento delle attività, l'esercizio dei poteri e l'adozione dei provvedimenti di cui al presente capo.

Art. 35.

Monitoraggio, analisi e supporto

1. Ai fini dell'articolo 7, l'Autorità nazionale competente NIS verifica e fornisce riscontro circa le informazioni trasmesse e la relativa corrispondenza ai requisiti prescritti per i soggetti registrati, ai fini dell'inserimento nell'elenco di cui all'articolo 7, comma 2, assicurando altresì adeguata pubblicità ai criteri concernenti l'ambito di applicazione del presente decreto e dei relativi obblighi.

2. L'Autorità nazionale competente NIS monitora l'attuazione degli obblighi di cui al presente decreto da parte dei soggetti che rientrano nell'ambito di applicazione di cui all'articolo 3, implementando, altresì, interventi di supporto per i soggetti medesimi.

3. L'Autorità nazionale competente NIS, ai fini dell'attività di monitoraggio di cui al comma 2, può:

a) richiedere ai soggetti una rendicontazione, anche periodica, ivi incluse autovalutazioni e piani di implementazione, dello stato di attuazione degli obblighi di cui al presente decreto, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali, dichiarando la finalità della richiesta;

b) richiedere ai soggetti l'esecuzione, periodica o mirata, di audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto;

c) richiedere ai soggetti l'esecuzione di scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

d) emanare raccomandazioni e avvertimenti relativi a presunte violazioni del presente decreto da parte dei soggetti interessati.

4. Ai fini del comma 2, l'Autorità nazionale competente NIS indica modalità e termini ragionevoli e proporzionati per adempiere, nonché per riferire circa lo stato di attuazione degli adempimenti.

5. L'Autorità nazionale competente NIS analizza le risultanze delle attività di cui al presente capo al fine di stabilire l'ordine di priorità degli interventi di supporto di cui al comma 2 nonché di individuare gli indirizzi di sviluppo della regolamentazione di cui all'articolo 31.

6. L'Autorità nazionale competente NIS implementa gli interventi di supporto di cui al comma 2 qualora ciò non costituisca un onere sproporzionato o eccessivo.

7. L'Autorità nazionale competente NIS, nello svolgimento delle attività di cui al presente capo, si può avvalere dei tavoli settoriali di cui all'articolo 11, comma 4, lettera *f)*.

Art. 36.

Verifiche e ispezioni

1. L'Autorità nazionale competente NIS, nell'esercizio dei poteri di verifica e ispettivi nei confronti dei soggetti che rientrano nell'ambito di applicazione del presente decreto, può sottoporre questi ultimi a:

a) verifiche della documentazione e delle informazioni trasmesse all'Autorità nazionale competente NIS ai sensi del presente decreto;

b) ispezioni in loco e a distanza, compresi controlli casuali;

c) richieste di accesso a dati, documenti e altre informazioni necessari allo svolgimento dei poteri di cui al presente articolo, dichiarando la finalità della richiesta e specificando le informazioni richieste ai soggetti.

2. Nei confronti dei soggetti importanti, i poteri di verifica e ispettivi si applicano unicamente qualora l'Autorità nazionale competente NIS acquisisca o riceva elementi di prova, indicazioni o informazioni che suggeriscano possibili violazioni del presente decreto.

Art. 37.

Misure di esecuzione

1. L'Autorità nazionale competente NIS, ai fini dell'esercizio dei suoi poteri di esecuzione, tiene anche conto degli esiti delle attività di monitoraggio, analisi e supporto di cui all'articolo 35 e delle risultanze dell'esercizio dei poteri di verifica e ispettivi di cui all'articolo 36.

2. L'Autorità nazionale competente NIS, nell'esercizio dei suoi poteri di esecuzione può richiedere ai soggetti, dichiarandone la finalità, di fornire i dati che dimostrino l'attuazione di politiche di sicurezza informatica, quali i risultati di audit sulla sicurezza e i relativi elementi di prova, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali anche ai fini:

a) della valutazione delle misure di gestione dei rischi per la sicurezza informatica;

b) del rispetto degli obblighi di trasmissione, comunicazione e notifica di cui al presente decreto.

3. L'Autorità nazionale competente NIS, nell'esercizio dei suoi poteri di esecuzione, può intimare ai soggetti:

a) di eseguire, su base periodica o mirata, audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto.

L'Autorità nazionale competente NIS non può prescrivere l'esecuzione periodica di audit di sicurezza ai soggetti importanti;

b) di eseguire scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con la medesima Autorità;

c) di attuare le raccomandazioni fornite in seguito a un audit sulla sicurezza;

d) di adempiere agli obblighi di cui al presente decreto;

e) di porre termine al comportamento che viola il presente decreto e di astenersi dal ripeterlo;

f) di attuare le istruzioni vincolanti impartite dalla medesima Autorità o di porre rimedio alle carenze individuate nell'adempimento degli obblighi di cui al presente decreto o alle conseguenze che derivano da violazioni del presente decreto;

g) ai fini dell'articolo 25, comma 9, di comunicare senza ingiustificato ritardo ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi;

h) ai fini dell'articolo 25, comma 10, di comunicare senza ingiustificato ritardo ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, qualsiasi misura o azione correttiva che tali destinatari possono adottare in risposta a tale minaccia, nonché, se opportuno, la minaccia informatica significativa stessa;

i) ai fini dell'articolo 25, comma 11, di informare il pubblico sugli incidenti occorsi;

l) di rendere pubbliche le violazioni di cui al presente decreto.

4. L'Agenzia per la cybersicurezza nazionale, nell'esercizio dei suoi poteri di esecuzione quale Autorità nazionale competente NIS, può intimare l'osservanza di istruzioni vincolanti per evitare il verificarsi di un incidente o per porvi rimedio.

5. L'Autorità nazionale competente NIS può designare un proprio funzionario per supportare il soggetto interessato ai fini dell'adempimento degli obblighi di cui al presente decreto, con compiti ben definiti nell'arco di un periodo di tempo determinato, anche tramite visite in loco e a distanza. Il soggetto interessato assicura la piena collaborazione con il funzionario designato.

6. Qualora il soggetto interessato non adempia alle disposizioni di cui ai commi 2, 3, 4 e 5, secondo periodo, l'Autorità nazionale competente NIS diffida il soggetto ad adempiere a tali disposizioni.

7. Ai fini dei commi 2, 3, 4 e 6, l'Autorità nazionale competente NIS indica modalità e termini ragionevoli e proporzionati per adempiere nonché per riferire circa lo stato di attuazione degli adempimenti.

8. Prima di adottare provvedimenti di cui ai commi 3 e 6, l'Autorità nazionale competente NIS notifica ai soggetti interessati le conclusioni preliminari, concedendo a questi ultimi un termine ragionevole, comunque non inferiore a quindici giorni, per presentare osservazioni.

9. Il comma 8 non trova applicazione nei casi in cui la notifica delle conclusioni preliminari non consenta azioni immediate per prevenire un incidente o rispondervi. In tali casi l'Autorità nazionale competente NIS motiva l'omissione della notifica di cui al comma 8.

10. Nei casi di adozione da parte dell'Autorità nazionale competente NIS di più provvedimenti successivi riconducibili alla medesima fattispecie, il comma 8 si applica esclusivamente al primo di questi provvedimenti.

Art. 38.

Sanzioni amministrative

1. L'Autorità nazionale competente NIS, ai fini dell'esercizio dei suoi poteri sanzionatori, tiene anche conto degli esiti delle attività di monitoraggio, supporto e analisi di cui all'articolo 35, delle risultanze dell'esercizio dei poteri di verifica e ispettivi di cui all'articolo 36, nonché dell'esercizio dei poteri di esecuzione di cui all'articolo 37.

2. Fermi restando i criteri di cui all'articolo 34, comma 6, l'Agenzia per la cybersicurezza nazionale con una o più determinazioni, adottate secondo le modalità dell'articolo 40, comma 5, può specificare laddove necessario i criteri per la determinazione dell'importo delle sanzioni per le violazioni di cui ai commi 8 e 10 del presente articolo, adottando tutte le misure necessarie per assicurarne l'effettività, la proporzionalità, la dissuasività e l'applicazione.

3. L'esercizio dei poteri di cui all'articolo 37 non impedisce la contestazione delle violazioni di cui ai commi 8 e 10 del presente articolo, nonché la relativa irrogazione di sanzioni amministrative di cui al presente articolo.

4. Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'articolo 37, commi 6 e 7, l'Autorità nazionale competente NIS può sospendere temporaneamente o chiedere a un organismo di certificazione o autorizzazione, oppure a un organo giurisdizionale, ai sensi della normativa vigente, di sospendere temporaneamente un certificato o un'autorizzazione relativi a una parte o alla totalità dei servizi o delle attività pertinenti svolti dal soggetto essenziale. Tale sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7. Le disposizioni di cui al presente comma non si applicano alle pubbliche amministrazioni di cui all'allegato III, nonché ai soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4.

5. Qualsiasi persona fisica responsabile di un soggetto essenziale o che agisca in qualità di suo rappresentante legale con l'autorità di rappresentarlo, di prendere decisioni per suo conto o di esercitare un controllo sul soggetto stesso, assicura il rispetto delle disposizioni di cui al presente decreto. Tali persone fisiche possono essere ritenute responsabili dell'inadempimento in caso di violazione del presente decreto da parte del soggetto di cui hanno rappresentanza.

6. Qualora il soggetto non adempia nei termini stabiliti dalla diffida di cui all'articolo 37, commi 6 e 7, l'Autorità nazionale competente NIS può disporre nei confronti delle persone fisiche di cui al comma 5 del presente articolo, ivi inclusi gli organi di amministrazione e gli organi direttivi di cui all'articolo 23 dei soggetti essenziali

e dei soggetti importanti, nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale di un soggetto essenziale o importante, l'applicazione della sanzione amministrativa accessoria della incapacità a svolgere funzioni dirigenziali all'interno del medesimo soggetto. Tale sospensione temporanea è applicata finché il soggetto interessato non adotta le misure necessarie a porre rimedio alle carenze o a conformarsi alle diffide di cui all'articolo 37, commi 6 e 7.

7. Ai dipendenti pubblici che esercitano i poteri di cui al comma 5, si applicano le norme in materia di responsabilità dei dipendenti pubblici e dei funzionari eletti o nominati. In particolare, la violazione degli obblighi di cui al presente decreto può costituire causa di responsabilità dirigenziale, disciplinare e amministrativo-contabile.

8. Con le sanzioni amministrative pecuniarie di cui al comma 9 sono punite le seguenti violazioni:

a) mancata osservanza degli obblighi imposti dall'articolo 23 agli organi di amministrazione e agli organi direttivi, nonché degli obblighi relativi alla gestione del rischio per la sicurezza informatica e alla notifica di incidente, di cui agli articoli 24 e 25, così come disciplinati ai sensi dell'articolo 31;

b) inottemperanza alle disposizioni adottate dall'Autorità nazionale competente NIS ai sensi dell'articolo 37, commi 3 e 4, e alle relative diffide.

9. Le violazioni di cui al comma 8 sono punite:

a) per i soggetti essenziali, escluse le pubbliche amministrazioni, con sanzioni amministrative pecuniarie fino a un massimo di euro 10.000.000 o del 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, se tale importo è superiore, il cui minimo è fissato nella misura di un ventesimo del massimo edittale;

b) per i soggetti importanti, escluse le pubbliche amministrazioni, con sanzioni amministrative pecuniarie fino a un massimo di euro 7.000.000 o dell'1,4% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE, se tale importo è superiore, il cui minimo è fissato nella misura di un trentesimo del massimo edittale;

c) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti essenziali, con sanzioni amministrative pecuniarie da euro 25.000 a euro 125.000;

d) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti importanti, le sanzioni amministrative pecuniarie di cui alla lettera *c)* sono ridotte di un terzo.

10. Con le sanzioni amministrative pecuniarie di cui al comma 11 sono punite le seguenti violazioni:

a) mancata registrazione, comunicazione o aggiornamento delle informazioni ai sensi dell'articolo 7, commi 1, 3, 4, 5 e 7;

b) inosservanza delle modalità stabilite dall'Autorità nazionale competente NIS ai sensi dell'articolo 7;

c) mancata comunicazione o aggiornamento dell'elenco delle attività e dei servizi nonché della loro categorizzazione ai sensi dell'articolo 30, comma 1;

d) mancata implementazione o attuazione degli obblighi relativi all'uso di schemi di certificazione, alla banca dei dati di registrazione dei nomi di dominio nonché alle previsioni settoriali specifiche di cui agli articoli 27, 29 e 32, così come disciplinati ai sensi dell'articolo 31.

e) mancata collaborazione con l'Autorità nazionale competente NIS nello svolgimento delle attività e nell'esercizio dei poteri di cui al presente capo;

f) mancata collaborazione con il CSIRT Italia.

11. Le violazioni di cui al comma 10, fermi restando i minimi edittali di cui al comma 9, sono punite:

a) per i soggetti essenziali, con sanzioni amministrative pecuniarie fino a un massimo dello 0,1% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE;

b) per i soggetti importanti, con sanzioni amministrative pecuniarie fino a un massimo dello 0,07% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, calcolato secondo le modalità previste della raccomandazione 2003/361/CE;

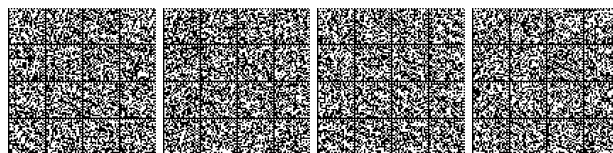
c) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti essenziali, con sanzioni amministrative pecuniarie da euro 10.000 a euro 50.000;

d) per le pubbliche amministrazioni di cui all'allegato III, nonché per i soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pubblico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, che sono soggetti importanti, le sanzioni amministrative pecuniarie di cui alla lettera *c)* sono ridotte di un terzo.

12. Si ha reiterazione delle violazioni di cui al presente articolo nei casi regolati dall'articolo 8-*bis* della legge 24 novembre del 1981, n. 689. Nei casi di reiterazione specifica, la sanzione prevista per la violazione è aumentata fino al doppio. Nei casi di reiterazione non specifica si applica la sanzione prevista per la violazione più grave aumentata fino al triplo.

13. In caso di mancata o tardiva registrazione di cui all'articolo 7, sono comunque contestate tutte le violazioni previste dai commi 8 e 10 del presente articolo, e si applica la sanzione prevista per la violazione più grave aumentata fino al triplo.

14. In caso di mancata osservanza degli obblighi relativi alla notifica di incidente di cui all'articolo 25, da parte delle pubbliche amministrazioni di cui all'allegato III, nonché dei soggetti rientranti fra le tipologie di cui all'allegato IV, punto 1, partecipati o sottoposti a controllo pub-

blico, e punto 4, laddove individuati secondo le modalità di cui all'articolo 40, comma 4, le disposizioni di cui al comma 9 del presente articolo si applicano solo in caso di reiterazione specifica nell'arco di cinque anni e l'Autorità nazionale competente NIS può esercitare, durante i dodici mesi successivi all'accertamento della violazione, i poteri di verifica e ispettivi di cui all'articolo 36.

15. Ai fini dell'attuazione del presente articolo, sono individuate, ai sensi dell'articolo 40, comma 1, lettera *c)*, le modalità di applicazione, nell'ambito del procedimento sanzionatorio, dei seguenti strumenti deflattivi del contenzioso:

a) l'invito a conformarsi che l'Autorità nazionale competente NIS, ove accerti la sussistenza delle violazioni, e fatto salvo il caso di reiterazione delle stesse, invia al trasgressore, assegnando un congruo termine perentorio, proporzionato al tipo e alla gravità della violazione, per conformare la condotta agli obblighi previsti dalla normativa vigente. Ove il trasgressore ottemperi all'obbligo di conformare la condotta nei termini previsti, il procedimento sanzionatorio non prosegue. La disposizione di cui alla presente lettera non si applica al soggetto che sia stato già destinatario della diffida di cui all'articolo 37, comma 6, ovvero ai soggetti e nei casi previsti dal comma 14 del presente articolo;

b) la facoltà di estinguere il procedimento attraverso il pagamento in misura ridotta pari alla terza parte del massimo della sanzione o se più favorevole, e qualora sia stabilito, al doppio del minimo della sanzione edittale, nel termine perentorio di sessanta giorni dalla data di notifica della contestazione. In caso di reiterazione si applica l'articolo 8-*bis* della legge 24 novembre 1981, n. 689;

c) le fattispecie in cui non è prevista pubblicità dell'irrogazione di sanzioni amministrative.

16. I proventi delle sanzioni amministrative pecuniarie irrogate dall'Autorità nazionale competente NIS ai sensi di quanto previsto dal presente decreto sono versati all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del decreto legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale.

Art. 39.

Assistenza reciproca

1. L'Autorità nazionale competente NIS coopera e assiste le autorità competenti degli altri Stati membri interessati, nonché può richiedere la cooperazione e l'assistenza reciproca alle medesime, in funzione delle necessità, nei seguenti casi:

a) un soggetto, considerato sotto la giurisdizione nazionale ai sensi dell'articolo 5 o i cui sistemi informativi e di rete sono ubicati sul territorio nazionale, fornisce servizi in uno o più altri Stati membri;

b) un soggetto, considerato sotto la giurisdizione di altri Stati membri ai sensi dell'articolo 5 o i cui sistemi informativi e di rete sono ubicati sul territorio di altri Stati membri, fornisce servizi sul territorio nazionale.

2. La cooperazione di cui al comma 1 comprende la reciproca:

a) notifica e consultazione, per il mezzo del Punto di contatto unico NIS, circa le attività ispettive, le misure di esecuzione e l'esercizio dei poteri sanzionatori, nonché la loro applicazione;

b) richiesta giustificata di attività ispettive o di adozione di misure di esecuzione;

c) assistenza proporzionata alle rispettive risorse affinché le attività ispettive e di esecuzione possano essere attuate in maniera efficace, efficiente e coerente.

3. L'assistenza reciproca di cui al comma 2, lettera *c)*, può riguardare richieste di informazioni e attività ispettive, comprese le richieste di effettuare ispezioni *in loco* o a distanza o audit sulla sicurezza mirati.

4. L'Autorità nazionale competente NIS può respingere una richiesta di assistenza da parte di autorità competenti degli altri Stati membri ai sensi del presente articolo quando:

a) l'Autorità nazionale competente NIS non è competente per fornire l'assistenza richiesta;

b) l'assistenza richiesta non è proporzionata ai compiti ispettivi e di esecuzione previsti dal presente decreto;

c) la richiesta riguarda informazioni o comporta attività che, se divulgate o svolte, sarebbero contrarie agli interessi essenziali di sicurezza nazionale, di pubblica sicurezza o di difesa dello Stato.

5. Ai fini del comma 4, prima di respingere una richiesta, l'Autorità nazionale competente NIS consulta le autorità competenti degli Stati membri interessati. Su richiesta di uno degli Stati membri interessati, l'Autorità nazionale competente NIS consulta anche la Commissione europea e l'ENISA.

6. Se opportuno e di comune accordo, l'Autorità nazionale competente NIS e le autorità competenti di altri Stati membri possono svolgere attività ispettive e di esecuzione comuni.

7. L'Autorità nazionale competente NIS può:

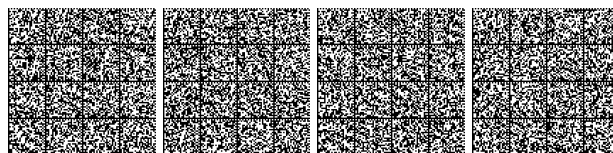
a) a fronte di una richiesta di assistenza reciproca da parte di autorità competenti di altri Stati membri, esercitare i poteri di cui al presente capo nei confronti di un soggetto che soddisfa i criteri di cui al comma 1, lettera *a)*, del presente articolo;

b) inoltrare una richiesta di assistenza reciproca alle autorità competenti degli altri Stati membri interessati per l'esercizio dei rispettivi poteri di cui al capo VII della direttiva 2022/2555 nei confronti di un soggetto che soddisfa i criteri di cui al comma 1, lettera *b)*, del presente articolo.

Capo VI

DISPOSIZIONI FINALI E TRANSITORIE

Art. 40.

Attuazione

1. Con uno o più decreti del Presidente del Consiglio dei ministri, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, su proposta dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'at-

tuazione della disciplina NIS di cui all'articolo 12 e previo parere del Comitato interministeriale per la cybersicurezza, di cui all'articolo 4 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109:

a) sono definiti i criteri per l'applicazione della clausola di salvaguardia di cui all'articolo 3, comma 4;

b) sono stabiliti i criteri, le procedure e le modalità di cui all'articolo 34, comma 10;

c) sono individuate le modalità di applicazione, nell'ambito del procedimento sanzionatorio, degli strumenti deflattivi del contenzioso di cui all'articolo 38, comma 15.

2. Con uno o più decreti del Presidente del Consiglio dei ministri, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, su proposta dell'Agenzia per la cybersicurezza nazionale, d'intesa con le Autorità di settore NIS interessate, sentito il Tavolo per l'attuazione della disciplina NIS e previo parere del Comitato interministeriale per la cybersicurezza:

a) possono essere stabiliti ulteriori criteri di identificazione delle tipologie di soggetto di cui agli allegati I e II, nonché delle ulteriori tipologie di soggetto di cui all'articolo 3;

b) possono essere individuate ulteriori categorie di pubbliche amministrazioni di cui all'articolo 3, commi 6 e 7, a cui si applica il presente decreto;

c) sono stabilite le modalità di raccordo e di collaborazione tra l'Agenzia per la cybersicurezza nazionale e le Autorità di settore NIS ai fini del presente decreto.

3. Con uno o più decreti del Presidente del Consiglio dei ministri, adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, su proposta dell'Agenzia per la cybersicurezza nazionale, d'intesa con le Amministrazioni interessate, sentito il Tavolo per l'attuazione della disciplina NIS, previo parere del Comitato interministeriale per la cybersicurezza, sono stabilite, ove necessario, le modalità di raccordo e collaborazione di cui all'articolo 14.

4. Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, su proposta delle Autorità di settore NIS interessate, sentito il Tavolo per l'attuazione della disciplina NIS:

a) sono individuati, ove necessario, i soggetti ai quali si applica la clausola di salvaguardia di cui all'articolo 3, comma 4;

b) sono individuati i soggetti ai quali si applica il presente decreto ai sensi dell'articolo 3, commi 8 e 9.

5. Con una o più determinazioni dell'Agenzia per la cybersicurezza nazionale, sentito il Tavolo per l'attuazione della disciplina NIS:

a) ai sensi degli articoli 3 e 6, è stabilito l'elenco dei soggetti essenziali e dei soggetti importanti di cui all'articolo 7, comma 2;

b) sono stabiliti i termini, le modalità nonché i procedimenti di utilizzo e accesso di cui all'articolo 7, comma 6, le eventuali ulteriori informazioni che i soggetti devono fornire ai sensi dei commi 1 e 4 del medesimo articolo, nonché i termini, le modalità e i procedimenti di designazione dei rappresentanti di cui all'articolo 5, comma 3;

c) possono essere definiti ulteriori disposizioni per l'organizzazione e per il funzionamento del Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12;

d) è adottata, d'intesa con il Ministero della giustizia, la politica nazionale di divulgazione coordinata delle vulnerabilità di cui all'articolo 16, comma 4;

e) possono essere imposte condizioni per le informazioni messe a disposizione dalle autorità competenti e dal CSIRT Italia nel contesto degli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all'articolo 17, comma 3;

f) sono stabilite le modalità con cui i soggetti essenziali e i soggetti importanti notificano all'Autorità nazionale competente NIS la loro partecipazione agli accordi di condivisione delle informazioni sulla sicurezza informatica di cui all'articolo 17, comma 4;

g) possono essere designati gli esperti di sicurezza informatica di cui all'articolo 21, comma 1, nonché individuate, se necessario, le modalità per l'esecuzione della revisione tra pari di cui al medesimo articolo 21;

h) può essere imposto l'utilizzo di prodotti TIC, servizi TIC e processi TIC certificati di cui all'articolo 27, definendo i relativi termini, criteri e modalità;

i) sono stabilite le categorie di rilevanza nonché le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi, a valenza multisettoriale e, ove opportuno, settoriale, di cui all'articolo 30;

l) sono stabiliti obblighi proporzionati e graduali, a valenza multisettoriale e, ove opportuno, settoriale, di cui all'articolo 31, le modalità di applicazione dei medesimi obblighi per i soggetti che svolgono attività in più settori o sottosettori e per i soggetti di cui all'articolo 32, commi 1 e 2;

m) sono stabiliti i criteri per la determinazione dell'importo delle sanzioni ai sensi dell'articolo 38, comma 2.

6. Sono esclusi dall'accesso e non sono soggetti a pubblicazione:

a) i decreti di cui al comma 3;

b) le determinazioni di cui al comma 4, lettera *b)*, e al comma 5, lettera *a)*;

c) atti, documenti, e informazioni relativi o comunque collegati alle notifiche degli incidenti o la cui divulgazione o il cui accesso possono comunque arrecare un possibile pregiudizio alla sicurezza nazionale nello spazio cibernetico.

7. Entro trenta giorni dalla data di entrata in vigore del presente decreto sono adottati:

a) i decreti del Presidente del Consiglio dei ministri di cui al comma 1, lettera *a)*, e al comma 3;

b) le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al comma 4, lettera *b)*, e al comma 5, lettere *b)* e *c)*.

8. Entro sei mesi dalla data di entrata in vigore del presente decreto, sono adottati:

a) i decreti del Presidente del Consiglio dei ministri di cui al comma 1, lettere *b)* e *c)*, e al comma 2, lettera *c)*;

b) le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al comma 5, lettere *d)*, *f)* e *l)*.

9. Entro diciotto mesi dalla data di entrata in vigore del presente decreto, sono adottate le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al comma 5, lettera *i)*.

10. I decreti del Presidente del Consiglio dei ministri di cui al presente articolo sono aggiornati periodicamente e, comunque, ogni tre anni.

11. Le determinazioni dell'Agenzia per la cybersicurezza nazionale di cui al presente articolo sono aggiornate periodicamente e, comunque, ogni due anni.

Art. 41.

Regime transitorio e abrogazioni

1. Le disposizioni di cui al presente decreto si applicano a decorrere dal 18 ottobre 2024.

2. A decorrere dal 18 ottobre 2024 il decreto legislativo 18 maggio 2018, n. 65, è abrogato, a esclusione dell'articolo 7, comma 8, e dell'articolo 8, comma 10, che sono abrogati dal 1° gennaio 2025. I capi IV e V del medesimo decreto legislativo n. 65 del 2018 continuano a trovare applicazione nei confronti dei soli soggetti di cui all'articolo 3, comma 9, lettera *a)*, fino alla data di adozione dei provvedimenti attuativi di cui all'articolo 40, commi 1, 2, 3, 4 e 5, lettere *a)*, *b)*, *e)* e *f)*.

3. Al codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259, sono apportate le seguenti modificazioni:

a) all'articolo 2, comma 1, la lettera *h)* è abrogata;

b) l'articolo 30, comma 26, e gli articoli 40 e 41 sono abrogati.

4. I provvedimenti attuativi degli articoli 40 e 41 del codice di cui al decreto legislativo n. 259 del 2003 continuano a trovare applicazione, per quanto non in contrasto con la legge e con le disposizioni del presente decreto, fino all'adozione delle determinazioni di cui all'articolo 40, comma 5, lettera *l)*.

Art. 42.

Fase di prima applicazione

1. In fase di prima applicazione:

a) ai sensi dell'articolo 7, entro il 17 gennaio 2025, i fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, fornitori di servizi di data center, fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network che rientrano nell'ambito di applicazione del presente decreto, si registrano sulla piattaforma digitale di cui all'articolo 7, comma 1;

b) sino al 31 dicembre 2025, il Tavolo per l'attuazione della disciplina NIS di cui all'articolo 12 si riunisce almeno una volta ogni sessanta giorni;

c) sino al 31 dicembre 2025, il termine per l'adempimento degli obblighi di cui all'articolo 25 è fissato in nove mesi dalla ricezione della comunicazione di cui all'articolo 7, comma 3, lettere *a)* e *b)*, e il termine per l'adempimento degli obblighi di cui agli articoli 23, 24 e 29 è fissato in diciotto mesi dalla medesima comunicazione. Ai fini di cui al primo periodo, l'Autorità nazionale competente NIS può stabilire modalità e specifiche di base per assicurare la conformità dei soggetti essenziali e dei soggetti importanti.

2. L'obbligo di cui all'articolo 30, comma 1, si applica a partire dal 1° gennaio 2026.

3. Ai sensi dell'articolo 7, comma 1, i soggetti essenziali e i soggetti importanti possono registrarsi a partire dalla data di pubblicazione della piattaforma di cui al medesimo comma.

Art. 43.

Modifiche normative

1. Al fine di assicurarne la coerenza con l'architettura nazionale di cybersicurezza e con i compiti dell'Agenzia per la cybersicurezza nazionale, al decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, sono apportate le seguenti modificazioni:

a) all'articolo 1, comma 1:

1) la lettera *d)* è sostituita dalla seguente:

«*d)* decreto legislativo NIS, il decreto legislativo di recepimento della direttiva (UE) 2022/2555, del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148;»;

2) alla lettera *e)*, le parole: «di cui all'articolo 6» sono sostituite dalle seguenti: «di cui all'articolo 9»;

b) all'articolo 7:

1) al comma 1:

1.1) la lettera *d)* è sostituita dalle seguenti:

«*d)* è Autorità nazionale competente NIS e Punto di contatto unico NIS di cui all'articolo 2, comma 1, lettere *d)* ed *e)*, del decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento;

d-*bis*) è Autorità nazionale di gestione delle crisi informatiche di cui all'articolo 2, comma 1, lettera *g)*, del decreto legislativo NIS;

d-*ter*) è CSIRT nazionale, denominato CSIRT Italia, di cui all'articolo 2, comma 1, lettera *i)*, del decreto legislativo NIS;»;

1.2) alla lettera *n)*, le parole: «CSIRT Italia di cui all'articolo 8» sono sostituite dalle seguenti «CSIRT Italia di cui all'articolo 2, comma 1, lettera *i)*»;

1.3) alla lettera n-*bis*), le parole: «di cui all'articolo 3, comma 1, lettere *g)* e *i)*» sono sostituite dalle seguenti: «i soggetti essenziali e i soggetti importanti di cui all'articolo 6 del decreto legislativo NIS»;

2) il comma 3 è abrogato;

c) l'articolo 15 è abrogato.

2. Per assicurare la coerenza con gli obblighi di cui al capo IV e con le disposizioni di cui al capo V del presente decreto, all'articolo 1 del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge del 18 novembre 2019, n. 133, sono apportate le seguenti modificazioni:

a) il comma 3-*bis* è abrogato;

b) il comma 8 è sostituito dal seguente:

«8. La notifica d'incidente ai sensi del comma 3, lettera *a)*, effettuata dai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che rientrano nell'ambito di applicazione del decreto legislativo di recepimento della direttiva (UE) 2022/2555 assolve agli obblighi in materia di notifica di incidente di cui all'articolo 25 del decreto legislativo medesimo.»;

c) dopo il comma 8, è inserito il seguente:

«8-*bis*. Ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che non sono individuati come soggetti essenziali o importanti ai sensi degli articoli 3 e 6 del decreto legislativo di recepimento della direttiva (UE) 2022/2555, si applicano gli obblighi di cui al capo IV e le attività ispettive e sanzionatorie di cui al capo V previste per i soggetti essenziali ai sensi del medesimo decreto legislativo, limitatamente ai sistemi informativi e di rete diversi da quelli inseriti nell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui all'articolo 1, comma 2, lettera *b)*, del presente decreto. L'Agenzia per la cybersicurezza nazionale, sentito il tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica, stabilisce con propria determina termini, modalità, specifiche e tempi graduali di implementazione degli obblighi di cui al presente comma.»;

d) il comma 17 è abrogato.

Art. 44.

Disposizioni finanziarie

1. Le spese ICT sostenute dalle pubbliche amministrazioni ai sensi degli articoli 10, 11, 13 e 15 del presente decreto e, più in generale le spese ICT sostenute per l'adeguamento dei sistemi informativi al presente decreto, sono coerenti con il Piano triennale per l'informatica nella pubblica amministrazione ai sensi dell'articolo 1, commi da 512 a 520, della legge 28 dicembre 2015, n. 208.

2. Agli oneri derivanti dagli articoli 10, comma 3, 11, comma 7, 13, comma 6, e 15 comma 8, pari a euro 409.424 per l'anno 2024 e euro 5.925.695 annui a decorrere dall'anno 2025, si provvede:

a) quanto euro a 409.424 per l'anno 2024, euro 2.625.695 per l'anno 2025, euro 2.707.695 per l'anno 2026 e euro 3.100.695 annui a decorrere dall'anno 2027, mediante corrispondente riduzione del Fondo per il recepimento della normativa europea di cui all'articolo 41-*bis* della legge 24 dicembre 2012, n. 234;

b) quanto a euro 3.300.000 per l'anno 2025, euro 3.218.000 per l'anno 2026 e euro 2.825.000 annui a decorrere dall'anno 2027, mediante utilizzo delle risorse rivenienti dall'abrogazione di cui al comma 2 dell'articolo 41.

3. Salvo quanto previsto dal comma 2, dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni competenti vi provvedono nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 4 settembre 2024

MATTARELLA

MELONI, *Presidente del Consiglio dei ministri*

FITTO, *Ministro per gli affari europei, il Sud, le politiche di coesione e il PNRR*

ZANGRILLO, *Ministro per la pubblica amministrazione*

TAJANI, *Ministro degli affari esteri e della cooperazione internazionale*

PIANTEDOSI, *Ministro dell'interno*

NORDIO, *Ministro della giustizia*

CROSETTO, *Ministro della difesa*

GIORGETTI, *Ministro dell'economia e delle finanze*

URSO, *Ministro delle imprese e del made in Italy*

LOLLOBRIGIDA, *Ministro dell'agricoltura, della sovranità alimentare e delle foreste*

PICHETTO FRATIN, *Ministro dell'ambiente e della sicurezza energetica*

SALVINI, *Ministro delle infrastrutture e dei trasporti*

BERNINI, *Ministro dell'università e della ricerca*

SANGIULIANO, *Ministro della cultura*

SCHILLACI, *Ministro della salute*

Visto, *il Guardasigilli:* NORDIO

SCHEMA DI DECRETO LEGISLATIVO DI RECEPIMENTO DELLA NIS2
Attuazione della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

ALLEGATO I
Settori ad altra criticità

Settore	Sottosettore	Tipologia di soggetto
1. Energia	a) Energia elettrica	— Impresa elettrica quale definita all'articolo 2, punto 57), della direttiva (UE) 2019/944 del Parlamento europeo e del Consiglio che esercita attività di «fornitura» quale definita all'articolo 2, punto 12), di tale direttiva
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 29), della direttiva (UE) 2019/944
		— Gestori del sistema di trasmissione quali definiti all'articolo 2, punto 35), della direttiva (UE) 2019/944
		— Produttori quali definiti all'articolo 2, punto 38), della direttiva (UE) 2019/944
		— Gestori del mercato elettrico designato quali definiti all'articolo 2, punto 8), del regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio
		— Partecipanti al mercato dell'energia elettrica quali definiti all'articolo 2, punto 25), del regolamento (UE) 2019/943 che forniscono servizi di aggregazione, gestione della domanda o stoccaggio di energia quali definiti all'articolo 2, punti 18), 20) e 59) della direttiva (UE) 2019/944
		— Gestori di un punto di ricarica responsabili della gestione e del funzionamento di un punto di ricarica che fornisce un servizio di ricarica a utenti finali, anche in nome e per conto di un fornitore di servizi di mobilità
	b) Teleriscaldamento e teleraffrescamento	— Gestori di teleriscaldamento o teleraffrescamento quali definiti all'articolo 2, punto 19), della direttiva (UE) 2018/2001 del Parlamento europeo e del Consiglio
	c) Petrolio	— Gestori di oleodotti
		— Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio
		— Organismi centrali di stoccaggio quali definiti all'articolo 2, lettera f), della direttiva 2009/119/CE del Consiglio
	d) Gas	— Imprese fornitrici quali definite all'articolo 2, punto 8), della direttiva 2009/73/CE del Parlamento europeo e del Consiglio
		— Gestori del sistema di distribuzione quali definiti all'articolo 2, punto 6), della direttiva 2009/73/CE

		— Gestori del sistema di trasporto quali definiti all'articolo 2, punto 4), della direttiva 2009/73/CE
		— Gestori dell'impianto di stoccaggio quali definiti all'articolo 2, punto 10), della direttiva 2009/73/CE
		— Gestori del sistema GNL quali definiti all'articolo 2, punto 12), della direttiva 2009/73/CE
		— Imprese di gas naturale quali definite all'articolo 2, punto 1), della direttiva 2009/73/CE;
		— Gestori di impianti di raffinazione e trattamento di gas naturale
	e) Idrogeno	— Gestori di impianti di produzione, stoccaggio e trasporto di idrogeno
2. Trasporti	a) Trasporto aereo	— Vettori aerei quali definiti all'articolo 3, punto 4), del regolamento (CE) n. 300/2008 utilizzati a fini commerciali
		— Gestori aeroportuali quali definiti all'articolo 2, punto 2), della direttiva 2009/12/CE del Parlamento europeo e del Consiglio, aeroporti quali definiti all'articolo 2, punto 1), di tale direttiva, compresi gli aeroporti centrali di cui all'allegato II, sezione 2, del regolamento (UE) n. 1315/2013 del Parlamento europeo e del Consiglio, e soggetti che gestiscono impianti annessi situati in aeroporti
		— Operatori attivi nel controllo della gestione del traffico che forniscono un servizio di controllo del traffico aereo quali definiti all'articolo 2, punto 1), del regolamento (CE) n. 549/2004 del Parlamento europeo e del Consiglio
	b) Trasporto ferroviario	— Gestori dell'infrastruttura quali definiti all'articolo 3, punto 2), della direttiva 2012/34/UE del Parlamento europeo e del Consiglio
		— Imprese ferroviarie quali definiti all'articolo 3, punto 1), della direttiva 2012/34/UE, compresi gli operatori degli impianti di servizio quali definiti all'articolo 3, punto 12), di tale direttiva
	c) Trasporto per vie d'acqua	— Compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci quali definite per il trasporto marittimo all'allegato I del regolamento (CE) n. 725/2004 del Parlamento europeo e del Consiglio, escluse le singole navi gestite da tale compagnia
		— Organi di gestione dei porti quali definiti all'articolo 3, punto 1), della direttiva 2005/65/CE del Parlamento europeo e del Consiglio, compresi i relativi impianti portuali quali definiti all'articolo 2, punto 11), del regolamento (CE) n. 725/2004, e soggetti che gestiscono opere e attrezzature all'interno di porti
		— Gestori di servizi di assistenza al traffico marittimo (VTS) quali definiti all'articolo 3, lettera o), della direttiva 2002/59/CE del Parlamento europeo e del Consiglio
	d) Trasporto su strada	— Autorità stradali quali definite all'articolo 2, punto 12), del regolamento delegato (UE) 2015/962 della Commissione responsabili del controllo della gestione del traffico, esclusi i soggetti pubblici per i

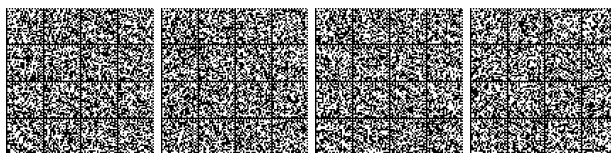
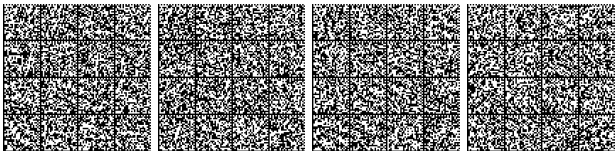
Settore	Sottosettore	Tipo di soggetto
		quali la gestione del traffico o la gestione di sistemi di trasporto intelligenti costituiscono soltanto una parte non essenziale della loro attività generale
		— Gestori di sistemi di trasporto intelligenti quali definiti all'articolo 4, punto 1), della direttiva 2010/40/UE del Parlamento europeo e del Consiglio
3. Settore bancario		Enti creditizi quali definiti all'articolo 4, punto 1), del regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio
4. Infrastrutture dei mercati finanziari		— Gestori delle sedi di negoziazione quali definiti all'articolo 4, punto 24), della direttiva 2014/65/UE del Parlamento europeo e del Consiglio
		— Controparti centrali (CCP) quali definite all'articolo 2, punto 1), del regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio
5. Settore sanitario		— Prestatori di assistenza sanitaria quali definiti all'articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio
		— Laboratori di riferimento dell'UE quali definiti all'articolo 15 del regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio
		— Soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti all'articolo 1, punto 2), della direttiva 2001/83/CE del Parlamento europeo e del Consiglio
		— Soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2
		— Soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'articolo 22 del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio
6. Acqua potabile		Fornitori e distributori di acque destinate al consumo umano, quali definiti all'articolo 2, punto 1, lettera a), della direttiva (UE) 2020/2184 del Parlamento europeo e del Consiglio, ma esclusi i distributori per i quali la distribuzione di acque destinate al consumo umano è una parte non essenziale dell'attività generale di distribuzione di altri prodotti e beni
7. Acque reflue		Imprese che raccolgono, smaltiscono o trattano acque reflue urbane, domestiche o industriali quali definite all'articolo 2, punti da 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, escluse le imprese per cui la raccolta, lo smaltimento o il trattamento di acque reflue urbane, domestiche o industriali è una parte non essenziale della loro attività generale
8. Infrastrutture digitali		— Fornitori di punti di interscambio internet

	— Fornitori di servizi di sistema dei nomi di dominio (*domain name system* – DNS), esclusi gli operatori dei server dei nomi radice
	— Gestori di registri dei nomi di dominio di primo livello (*top level domain* – TLD)
	— Fornitori di servizi di cloud computing
	— Fornitori di servizi di data center
	— Fornitori di reti di distribuzione dei contenuti (*content delivery network*)
	— Prestatori di servizi fiduciari
	— Fornitori di reti pubbliche di comunicazione elettronica
	— Fornitori di servizi di comunicazione elettronica accessibili al pubblico
9. Gestione dei servizi TIC (business-to-business)	— Fornitori di servizi gestiti
	— Fornitori di servizi di sicurezza gestiti
10. Spazio	Operatori di infrastrutture terrestri possedute, gestite e operate dagli Stati membri o da privati, che sostengono la fornitura di servizi spaziali, esclusi i fornitori di reti pubbliche di comunicazione elettronica

SCHEMA DI DECRETO LEGISLATIVO DI RECEPIMENTO DELLA NIS2

Attuazione della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

ALLEGATO II
Altri settori critici

Settore	Sottosettore	Tipologia di soggetto
1. Servizi postali e di corriere		Fornitori di servizi postali quali definiti all'articolo 2, punto 1 bis), della direttiva 97/67/CE, tra cui i fornitori di servizi di corriere
2. Gestione dei rifiuti		Imprese che si occupano della gestione dei rifiuti quali definite all'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, escluse quelle per cui la gestione dei rifiuti non è la principale attività economica
3. Fabbricazione, produzione e distribuzione di sostanze chimiche		Imprese che si occupano della fabbricazione di sostanze e della distribuzione di sostanze o miscele di cui all'articolo 3, punti 9) e 14), del regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio e imprese che si occupano della produzione di articoli quali definite all'articolo 3, punto 3), del medesimo regolamento, da sostanze o miscele
4. Produzione, trasformazione e distribuzione di alimenti		Imprese alimentari quali definite all'articolo 3, punto 2), del regolamento (CE) n. 178/2002 del Parlamento europeo e del Consiglio che si occupano della distribuzione all'ingrosso e della produzione industriale e trasformazione
5. Fabbricazione	a) Fabbricazione di dispositivi medici e di dispositivi medico-diagnostici in vitro	Soggetti che fabbricano dispositivi medici quali definiti all'articolo 2, punto 1), del regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio e soggetti che fabbricano dispositivi medico-diagnostici in vitro quali definiti all'articolo 2, punto 2), del regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio ad eccezione dei soggetti che fabbricano dispositivi medici di cui all'allegato I, punto 5), quinto trattino, della presente direttiva
	b) Fabbricazione di computer e prodotti di elettronica e ottica	Imprese che svolgono attività economiche di cui alla sezione C, divisione 26, della NACE Rev. 2
	c) Fabbricazione di apparecchiature elettriche	Imprese che svolgono attività economiche di cui alla sezione C, divisione 27, della NACE Rev. 2
	d) Fabbricazione di macchinari e apparecchiature n.c.a.	Imprese che svolgono attività economiche di cui alla sezione C, divisione 28, della NACE Rev. 2

	e) Fabbricazione di autoveicoli, rimorchi e semirimorchi	Imprese che svolgono attività economiche di cui alla sezione C, divisione 29, della NACE Rev. 2
	f) Fabbricazione di altri mezzi di trasporto	Imprese che svolgono attività economiche di cui alla sezione C, divisione 30, della NACE Rev. 2
6. Fornitori di servizi digitali		— Fornitori di mercati online
		— Fornitori di motori di ricerca online
		— Fornitori di piattaforme di social network
		— Fornitori di servizi di registrazione dei nomi di dominio
7. Ricerca		Organizzazioni di ricerca

SCHEMA DI DECRETO LEGISLATIVO DI RECEPIMENTO DELLA NIS2

Attuazione della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

ALLEGATO III

Amministrazioni centrali, regionali, locali e di altro tipo

1. Ai fini dell'articolo 3, comma 6, sono individuatele seguenti categorie:

a) amministrazioni centrali:

1) gli Organi costituzionali e di rilievo costituzionale;
2) la Presidenza del Consiglio dei ministri e i Ministeri;
3) le Agenzie fiscali;
4) le Autorità amministrative indipendenti;

b) amministrazioni regionali:

1. le Regioni e le Province autonome.

c) amministrazioni locali

1. le Città metropolitane;
2. i Comuni con popolazione superiore a 100.000 abitanti;
3. i Comuni capoluoghi di regione;
4. le Aziende sanitarie locali.

d) altri soggetti pubblici:

1. gli Enti di regolazione dell'attività economica;
2. gli Enti produttori di servizi economici;
3. gli Enti a struttura associativa;
4. gli Enti produttori di servizi assistenziali, ricreativi e culturali;
5. gli Enti e le Istituzioni di ricerca;
6. gli Istituti zooprofilattici sperimentali.

SCHEMA DI DECRETO LEGISLATIVO DI RECEPIMENTO DELLA NIS2
Attuazione della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di sicurezza informatica nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148

ALLEGATO IV
Ulteriori tipologie di soggetti

1. Soggetti che forniscono servizi di trasporto pubblico locale.
2. Istituti di istruzione che svolgono attività di ricerca.
3. Soggetti che svolgono attività di interesse culturale.
4. Società *in house*, società partecipate e società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175.

NOTE

AVVERTENZA:

Il testo delle note qui pubblicato è stato redatto dall'amministrazione competente per materia, ai sensi dell'art. 10, commi 2 e 3, del testo unico delle disposizioni sulla promulgazione delle leggi, sull'emanazione dei decreti del Presidente della Repubblica e sulle pubblicazioni ufficiali della Repubblica italiana, approvato con D.P.R. 28 dicembre 1985, n. 1092, al solo fine di facilitare la lettura delle disposizioni di legge, modificate o alle quali è operato il rinvio. Restano invariati il valore e l'efficacia degli atti legislativi qui trascritti.

Per le direttive CEE vengono forniti gli estremi di pubblicazione nella *Gazzetta Ufficiale* delle Comunità europee (GUUE).

Note alle premesse:

L'art. 76 della Costituzione stabilisce che l'esercizio della funzione legislativa non può essere delegato al Governo se non con determinazione di principi e criteri direttivi e soltanto per tempo limitato e per oggetti definiti.

L'art. 87, quinto comma, della Costituzione conferisce al Presidente della Repubblica il potere di promulgare le leggi ed emanare i decreti aventi valore di legge e i regolamenti.

— Si riporta l'articolo 14 della legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri), pubblicata nella *Gazzetta Ufficiale* 12 settembre 1988, n. 214, S.O. :

«Art. 14 *(Decreti legislativi)*. — 1. I decreti legislativi adottati dal Governo ai sensi dell'articolo 76 della Costituzione sono emanati dal Presidente della Repubblica con la denominazione di "decreto legislativo" e con l'indicazione, nel preambolo, della legge di delegazione, della deliberazione del Consiglio dei ministri e degli altri adempimenti del procedimento prescritti dalla legge di delegazione.

2. L'emanazione del decreto legislativo deve avvenire entro il termine fissato dalla legge di delegazione; il testo del decreto legislativo adottato dal Governo è trasmesso al Presidente della Repubblica, per la emanazione, almeno venti giorni prima della scadenza.

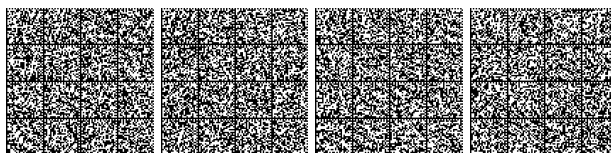
3. Se la delega legislativa si riferisce ad una pluralità di oggetti distinti suscettibili di separata disciplina, il Governo può esercitarla mediante più atti successivi per uno o più degli oggetti predetti. In relazione al termine finale stabilito dalla legge di delegazione, il Governo informa periodicamente le Camere sui criteri che segue nell'organizzazione dell'esercizio della delega.

4. In ogni caso, qualora il termine previsto per l'esercizio della delega ecceda in due anni, il Governo è tenuto a richiedere il parere delle Camere sugli schemi dei decreti delegati. Il parere è espresso dalle Commissioni permanenti delle due Camere competenti per materia entro sessanta giorni, indicando specificamente le eventuali disposizioni non ritenute corrispondenti alle direttive della legge di delegazione. Il Governo, nei trenta giorni successivi, esaminato il parere, ritrasmette, con le sue osservazioni e con eventuali modificazioni, i testi alle Commissioni per il parere definitivo che deve essere espresso entro trenta giorni.».

— Si riportano gli articoli 31 e 32 della legge 24 dicembre 2012, n. 234 (Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea), pubblicata nella *Gazzetta Ufficiale* 4 gennaio 2013, n. 3:

«Art. 31 *(Procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea)*. — 1. In relazione alle deleghe legislative conferite con la legge di delegazione europea per il recepimento delle direttive, il Governo adotta i decreti legislativi entro il termine di quattro mesi antecedenti a quello di recepimento indicato in ciascuna delle direttive; per le direttive il cui termine così determinato sia già scaduto alla data di entrata in vigore della legge di delegazione europea, ovvero scada nei tre mesi successivi, il Governo adotta i decreti legislativi di recepimento entro tre mesi dalla data di entrata in vigore della medesima legge; per le direttive che non prevedono un termine di recepimento, il Governo adotta i relativi decreti legislativi entro dodici mesi dalla data di entrata in vigore della legge di delegazione europea.

2. I decreti legislativi sono adottati, nel rispetto dell'articolo 14 della legge 23 agosto 1988, n. 400, su proposta del Presidente del Consiglio dei Ministri o del Ministro per gli affari europei e del Ministro con competenza prevalente nella materia, di concerto con i Ministri degli affari esteri, della giustizia, dell'economia e delle finanze e con gli altri Ministri interessati in relazione all'oggetto della direttiva. I decreti legislativi sono accompagnati da una tabella di concordanza tra le disposizioni in essi previste e quelle della direttiva da recepire, predisposta dall'amministrazione con competenza istituzionale prevalente nella materia.

3. La legge di delegazione europea indica le direttive in relazione alle quali sugli schemi dei decreti legislativi di recepimento è acquisito il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica. In tal caso gli schemi dei decreti legislativi sono trasmessi, dopo l'acquisizione degli altri pareri previsti dalla legge, alla Camera dei deputati e al Senato della Repubblica affinché su di

essi sia espresso il parere delle competenti Commissioni parlamentari. Decorsi quaranta giorni dalla data di trasmissione, i decreti sono emanati anche in mancanza del parere. Qualora il termine per l'espressione del parere parlamentare di cui al presente comma ovvero i diversi termini previsti dai commi 4 e 9 scadano nei trenta giorni che precedono la scadenza dei termini di delega previsti ai commi 1 o 5 o successivamente, questi ultimi sono prorogati di tre mesi.

4. Gli schemi dei decreti legislativi recanti recepimento delle direttive che comportino conseguenze finanziarie sono corredati della relazione tecnica di cui all'articolo 17, comma 3, della legge 31 dicembre 2009, n. 196. Su di essi è richiesto anche il parere delle Commissioni parlamentari competenti per i profili finanziari. Il Governo, ove non intenda conformarsi alle condizioni formulate con riferimento all'esigenza di garantire il rispetto dell'articolo 81, quarto comma, della Costituzione, ritrasmette alle Camere i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle Commissioni parlamentari competenti per i profili finanziari, che devono essere espressi entro venti giorni.

5. Entro ventiquattro mesi dalla data di entrata in vigore di ciascuno dei decreti legislativi di cui al comma 1, nel rispetto dei principi e criteri direttivi fissati dalla legge di delegazione europea, il Governo può adottare, con la procedura indicata nei commi 2, 3 e 4, disposizioni integrative e correttive dei decreti legislativi emanati ai sensi del citato comma 1, fatto salvo il diverso termine previsto dal comma 6.

6. Con la procedura di cui ai commi 2, 3 e 4 il Governo può adottare disposizioni integrative e correttive di decreti legislativi emanati ai sensi del comma 1, al fine di recepire atti delegati dell'Unione europea di cui all'articolo 290 del Trattato sul funzionamento dell'Unione europea, che modificano o integrano direttive recepite con tali decreti legislativi. Le disposizioni integrative e correttive di cui al primo periodo sono adottate nel termine di cui al comma 5 o nel diverso termine fissato dalla legge di delegazione europea. Resta ferma la disciplina di cui all'articolo 36 per il recepimento degli atti delegati dell'Unione europea che recano meri adeguamenti tecnici.

7. I decreti legislativi di recepimento delle direttive previste dalla legge di delegazione europea, adottati, ai sensi dell'articolo 117, quinto comma, della Costituzione, nelle materie di competenza legislativa delle regioni e delle province autonome, si applicano alle condizioni e secondo le procedure di cui all'articolo 41, comma 1.

8. I decreti legislativi adottati ai sensi dell'articolo 33 e attinenti a materie di competenza legislativa delle regioni e delle province autonome sono emanati alle condizioni e secondo le procedure di cui all'articolo 41, comma 1.

9. Il Governo, quando non intende conformarsi ai pareri parlamentari di cui al comma 3, relativi a sanzioni penali contenute negli schemi di decreti legislativi recanti attuazione delle direttive, ritrasmette i testi, con le sue osservazioni e con eventuali modificazioni, alla Camera dei deputati e al Senato della Repubblica. Decorsi venti giorni dalla data di ritrasmissione, i decreti sono emanati anche in mancanza di nuovo parere.»

«Art. 32 *(Principi e criteri direttivi generali di delega per l'attuazione del diritto dell'Unione europea)*. — 1. Salvi gli specifici principi e criteri direttivi stabiliti dalla legge di delegazione europea e in aggiunta a quelli contenuti nelle direttive da attuare, i decreti legislativi di cui all'articolo 31 sono informati ai seguenti principi e criteri direttivi generali:

a) le amministrazioni direttamente interessate provvedono all'attuazione dei decreti legislativi con le ordinarie strutture amministrative, secondo il principio della massima semplificazione dei procedimenti e delle modalità di organizzazione e di esercizio delle funzioni e dei servizi;

b) ai fini di un migliore coordinamento con le discipline vigenti per i singoli settori interessati dalla normativa da attuare, sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione normativi con l'indicazione esplicita delle norme abrogate, fatti salvi i procedimenti oggetto di semplificazione amministrativa ovvero le materie oggetto di delegificazione;

c) gli atti di recepimento di direttive dell'Unione europea non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse, ai sensi dell'articolo 14, commi 24-*bis*, 24-*ter* e 24-*quater*, della legge 28 novembre 2005, n. 246;

d) al di fuori dei casi previsti dalle norme penali vigenti, ove necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste sanzioni amministrative e penali per le infrazioni alle disposizioni dei decreti stessi. Le sanzioni penali, nei limiti, rispettivamente, dell'ammenda fino a 150.000 euro e dell'arresto fino a tre anni, sono previste, in via alternativa o congiunta, solo nei casi in cui le infrazioni ledano o espongano a pericolo interessi costituzionalmente protetti. In tali casi sono previste: la pena dell'ammenda alternativa all'arresto per le infrazioni che espongano a pericolo o danneggino l'interesse protetto; la pena dell'arresto congiunta a quella dell'ammenda per le infrazioni che rechino un danno di particolare gravità. Nelle predette ipotesi, in luogo dell'arresto e dell'ammenda, possono essere previste anche le sanzioni alternative di cui agli articoli 53 e seguenti del decreto legislativo 28 agosto 2000, n. 274, e la relativa competenza del giudice di pace. La sanzione amministrativa del pagamento di una somma non inferiore a 150 euro e non superiore a 150.000 euro è prevista per le infrazioni che ledono o espongono a pericolo interessi diversi da quelli indicati dalla presente lettera. Nell'ambito dei limiti minimi e massimi previsti, le sanzioni indicate dalla presente lettera sono determinate nella loro entità, tenendo conto della diversa potenzialità lesiva dell'interesse protetto che ciascuna infrazione presenta in astratto, di specifiche qualità personali del colpevole, comprese quelle che impongono particolari doveri di prevenzione, controllo o vigilanza, nonché del vantaggio patrimoniale che l'infrazione può recare al colpevole ovvero alla persona o all'ente nel cui interesse egli agisce. Ove necessario per assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste inoltre le sanzioni amministrative accessorie della sospensione fino a sei mesi e, nei casi più gravi, della privazione definitiva di facoltà e diritti derivanti da provvedimenti dell'amministrazione, nonché sanzioni penali accessorie nei limiti stabiliti dal codice penale. Al medesimo fine è prevista la confisca obbligatoria delle cose che servirono o furono destinate a commettere l'illecito amministrativo o il reato previsti dai medesimi decreti legislativi, nel rispetto dei limiti stabiliti dall'articolo 240, terzo e quarto comma, del codice penale e dall'articolo 20 della legge 24 novembre 1981, n. 689, e successive modificazioni. Entro i limiti di pena indicati nella presente lettera sono previste sanzioni anche accessorie identiche a quelle eventualmente già comminate dalle leggi vigenti per violazioni omogenee e di pari offensività rispetto alle infrazioni alle disposizioni dei decreti legislativi. Nelle materie di cui all'articolo 117, quarto comma, della Costituzione, le sanzioni amministrative sono determinate dalle regioni;

e) al recepimento di direttive o all'attuazione di altri atti dell'Unione europea che modificano precedenti direttive o atti già attuati con legge o con decreto legislativo si procede, se la modificazione non comporta ampliamento della materia regolata, apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione della direttiva o di altro atto modificato;

f) nella redazione dei decreti legislativi di cui all'articolo 31 si tiene conto delle eventuali modificazioni delle direttive dell'Unione europea comunque intervenute fino al momento dell'esercizio della delega;

g) quando si verifichino sovrapposizioni di competenze tra amministrazioni diverse o comunque siano coinvolte le competenze di più amministrazioni statali, i decreti legislativi individuano, attraverso le più opportune forme di coordinamento, rispettando i principi di sussidiarietà, differenziazione, adeguatezza e leale collaborazione e le competenze delle regioni e degli altri enti territoriali, le procedure per salvaguardare l'unitarietà dei processi decisionali, la trasparenza, la celerità, l'efficacia e l'economicità nell'azione amministrativa e la chiara individuazione dei soggetti responsabili;

h) qualora non siano di ostacolo i diversi termini di recepimento, vengono attuate con un unico decreto legislativo le direttive che riguardano le stesse materie o che comunque comportano modifiche degli stessi atti normativi;

i) è assicurata la parità di trattamento dei cittadini italiani rispetto ai cittadini degli altri Stati membri dell'Unione europea e non può essere previsto in ogni caso un trattamento sfavorevole dei cittadini italiani.»

— Si riporta l'articolo 3 della legge 21 febbraio 2024, n. 15 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea - Legge di delegazione europea 2022-2023), pubblicata nella *Gazzetta Ufficiale* 24 febbraio 2024, n. 46:

«Art. 3. *(Princìpi e criteri direttivi per l'esercizio della delega per il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2))*. — 1. Nell'esercizio della delega per il recepimento della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre

2022, il Governo, sentita l'Agenzia per la cybersicurezza nazionale, osserva, oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti princìpi e criteri direttivi specifici:

a) individuare i criteri in base ai quali un ente pubblico può essere considerato pubblica amministrazione ai fini dell'applicazione delle disposizioni della direttiva (UE) 2022/2555, anche considerando la possibilità di applicazione della direttiva medesima ai comuni e alle province secondo princìpi di gradualità, proporzionalità e adeguatezza;

b) escludere dall'ambito di applicazione delle disposizioni della direttiva (UE) 2022/2555 gli enti della pubblica amministrazione operanti nei settori di cui all'articolo 2, paragrafo 7, della direttiva medesima, compresi gli organismi di informazione per la sicurezza ai quali si applicano le disposizioni della legge 3 agosto 2007, n. 124;

c) avvalersi della facoltà di cui all'articolo 2, paragrafo 8, della direttiva (UE) 2022/2555, prevedendo che con uno o più decreti del Presidente del Consiglio dei ministri, adottati su proposta delle competenti amministrazioni, siano esentati soggetti specifici che svolgono attività nei settori ivi indicati o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui all'articolo 2, paragrafo 7, della medesima direttiva;

d) confermare la distinzione tra l'Agenzia per la cybersicurezza nazionale, quale autorità nazionale competente e punto di contatto, ai sensi dell'articolo 8 della direttiva (UE) 2022/2555, e le autorità di settore operanti negli ambiti di cui agli allegati I e II alla medesima direttiva;

e) in relazione all'istituzione del team di risposta agli incidenti di sicurezza informatica (CSIRT), di cui all'articolo 10 della direttiva (UE) 2022/2555, confermare le disposizioni dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65, in materia di istituzione del CSIRT Italia, nonché ampliare quanto previsto dal medesimo decreto legislativo prevedendo la collaborazione tra tutte le strutture pubbliche con funzioni di Computer Emergency Response Team (CERT) coinvolte in caso di eventi malevoli per la sicurezza informatica;

f) prevedere un regime transitorio per i soggetti già sottoposti alla disciplina del decreto legislativo 18 maggio 2018, n. 65, recante attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, garantendo termini congrui di adeguamento, ai fini della migliore applicazione delle disposizioni previste dalla direttiva (UE) 2022/2555;

g) prevedere meccanismi che consentano la registrazione dei soggetti essenziali e importanti, di cui all'articolo 3 della direttiva (UE) 2022/2555, per la comunicazione dei dati previsti dal paragrafo 4 del medesimo articolo 3, compresi i soggetti che gestiscono servizi connessi o strumentali alle attività oggetto delle disposizioni della direttiva medesima relative al settore della cultura;

h) in relazione alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555, prevedere l'individuazione, attraverso l'utilizzo di strumenti flessibili atti a corrispondere al rapido sviluppo tecnologico, delle tecnologie necessarie ad assicurare l'effettiva attivazione delle misure stesse. L'autorità amministrativa individuata come responsabile di tale procedimento provvede altresì all'aggiornamento degli strumenti adottati;

i) introdurre nella legislazione vigente, anche in materia penale, le modifiche necessarie al fine di assicurare il corretto recepimento nell'ordinamento nazionale delle disposizioni della direttiva (UE) 2022/2555 in materia di divulgazione coordinata delle vulnerabilità;

l) definire le competenze dell'Agenzia per l'Italia digitale e dell'Agenzia per la cybersicurezza nazionale in relazione alle attività previste dal regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014;

m) individuare criteri oggettivi e proporzionati ai fini dell'applicazione degli obblighi informativi di cui all'articolo 23, paragrafo 2, della direttiva (UE) 2022/2555;

n) rivedere il sistema sanzionatorio e il sistema di vigilanza ed esecuzione, in particolare:

1) prevedendo sanzioni effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla direttiva (UE) 2022/2555, anche in deroga ai criteri e ai limiti previsti dall'articolo 32, comma 1, lettera *d)*, della legge 24 dicembre 2012, n. 234, e alla legge 24 novembre 1981, n. 689, introducendo strumenti deflativi del contenzioso, quali la diffida ad adempiere;

2) prevedendo che gli introiti derivanti dall'irrogazione delle sanzioni siano versati all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale;

o) assicurare il migliore coordinamento tra le disposizioni adottate ai sensi del presente articolo per il recepimento della direttiva (UE) 2022/2555, le disposizioni adottate ai sensi dell'articolo 5 della presente legge per il recepimento della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché le disposizioni del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, e quelle adottate ai sensi dell'articolo 16 della presente legge per l'adeguamento a quest'ultimo e per il recepimento della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

p) apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione del presente articolo.».

— La direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 è pubblicata nella GUUE n. 17 del 27 dicembre 2022, serie L.

— La comunicazione della Commissione, del 13 settembre 2023, relativa all'applicazione dell'articolo 4, paragrafi 1 e 2, della direttiva (UE) 2022/2555 è pubblicata nella GUUE n. 328 del 18 settembre 2023, serie C;

— La direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) è pubblicata nella G.U.C.E. 31 luglio 2002, n. 201, serie L;

— Il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE è pubblicato nella GUUE del 28 agosto 2014 n. 257, serie L;

— Il regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale è pubblicato nella GUUE del 30 aprile 2024 serie L;

— Il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») è pubblicato nella GUUE del 7 giugno 2019 151 serie L;

— La raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese è pubblicata nella Gazzetta Ufficiale dell'Unione Europea del 20 maggio 2003, n. 124, serie L.

— La direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio è pubblicata nella Gazzetta Ufficiale dell'Unione Europea del 14 agosto 2013;

— Il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 è pubblicato nella GUUE del 27 dicembre 2022 n. 133 serie L;

— La direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario è pubblicata nella GUUE del 27 dicembre 2022 n. 333;

— La direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio è pubblicata nella GUUE del 27 dicembre 2022 n. 333, serie L;

— Si riportano gli articoli 1 e 2 del decreto legislativo 23 giugno 2011, n. 118 (Disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42), pubblicato nella *Gazzetta Ufficiale* 26 luglio 2011, n. 172:

«Art. 1 *(Oggetto e ambito di applicazione)*. — 1. Ai sensi dell'art. 117, secondo comma, lettera *e)*, della Costituzione, il presente titolo e il titolo III disciplinano l'armonizzazione dei sistemi contabili e degli schemi di bilancio delle Regioni, ad eccezione dei casi in cui il Titolo II disponga diversamente, con particolare riferimento alla fattispecie di cui all'art. 19, comma 2, lettera *b)*, degli enti locali di cui all'art. 2 del decreto legislativo 18 agosto 2000, n. 267, e dei loro enti e organismi strumentali, esclusi gli enti di cui al titolo II del presente decreto. A decorrere dal 1° gennaio 2015 cessano di avere efficacia le disposizioni legislative regionali incompatibili con il presente decreto.

2. Ai fini del presente decreto:

a) per enti strumentali si intendono gli enti di cui all'art. 11-*ter*, distinti nelle tipologie definite in corrispondenza delle missioni del bilancio;

b) per organismi strumentali delle regioni e degli enti locali si intendono le loro articolazioni organizzative, anche a livello territoriale, dotate di autonomia gestionale e contabile, prive di personalità giuridica. Le gestioni fuori bilancio autorizzate da legge e le istituzioni di cui all'art. 114, comma 2, del decreto legislativo 18 agosto 2000, n. 267, sono organismi strumentali. Gli organismi strumentali sono distinti nelle tipologie definite in corrispondenza delle missioni del bilancio.

3.

4.

5. Per gli enti coinvolti nella gestione della spesa sanitaria finanziata con le risorse destinate al Servizio sanitario nazionale, come individuati all'articolo 19, si applicano le disposizioni recate dal Titolo II.»

«Art. 2 *(Adozione di sistemi contabili omogenei)*. — 1. Le Regioni e gli enti locali di cui all'articolo 2 del decreto legislativo 18 agosto 2000, n. 267 adottano la contabilità finanziaria cui affiancano, ai fini conoscitivi, un sistema di contabilità economico-patrimoniale, garantendo la rilevazione unitaria dei fatti gestionali sia sotto il profilo finanziario che sotto il profilo economico-patrimoniale.

2. Gli enti strumentali delle amministrazioni di cui al comma 1 che adottano la contabilità finanziaria affiancano alla stessa, ai fini conoscitivi, un sistema di contabilità economico-patrimoniale, garantendo la rilevazione unitaria dei fatti gestionali, sia sotto il profilo finanziario che sotto il profilo economico-patrimoniale.

3. Le istituzioni degli enti locali di cui all'articolo 114 del decreto legislativo 18 agosto 2000, n. 267 e gli altri organismi strumentali delle amministrazioni pubbliche di cui al comma 1 adottano il medesimo sistema contabile dell'amministrazione di cui fanno parte.

4.»

— Si riporta l'articolo 19 del decreto-legge 22 giugno 2012, n. 83 (Misure urgenti per la crescita del Paese), convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, pubblicato nella *Gazzetta Ufficiale* 26 giugno 2012, n. 147, S.O.:

«Art. 19 *(Istituzione dell'Agenzia per l'Italia digitale)*. — 1. È istituita l'Agenzia per l'Italia Digitale, sottoposta alla vigilanza del Presidente del Consiglio dei Ministri o del Ministro da lui delegato.

2. L'Agenzia opera sulla base di principi di autonomia organizzativa, tecnico-operativa, gestionale, di trasparenza e di economicità e persegue gli obiettivi di efficacia, efficienza, imparzialità, semplificazione e partecipazione dei cittadini e delle imprese. Per quanto non previsto dal presente decreto all'Agenzia si applicano gli articoli 8 e 9 del decreto legislativo 30 luglio 1999, n. 300.».

— Si riporta l'articolo 3 della legge L. 21 febbraio 2024, n. 15 (Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2022-2023), pubblicata nella *Gazzetta Ufficiale* 24 febbraio 2024, n. 46:

«Art. 3 *(Princìpi e criteri direttivi per l'esercizio della delega per il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2))*. — 1. Nell'esercizio della delega per il recepimento della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, il Governo, sentita l'Agenzia per la cybersicurezza nazionale, osserva, oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti princìpi e criteri direttivi specifici:

a) individuare i criteri in base ai quali un ente pubblico può essere considerato pubblica amministrazione ai fini dell'applicazione delle disposizioni della direttiva (UE) 2022/2555, anche considerando la possibilità di applicazione della direttiva medesima ai comuni e alle province secondo princìpi di gradualità, proporzionalità e adeguatezza;

b) escludere dall'ambito di applicazione delle disposizioni della direttiva (UE) 2022/2555 gli enti della pubblica amministrazione operanti nei settori di cui all'articolo 2, paragrafo 7, della direttiva medesima, compresi gli organismi di informazione per la sicurezza ai quali si applicano le disposizioni della legge 3 agosto 2007, n. 124;

c) avvalersi della facoltà di cui all'articolo 2, paragrafo 8, della direttiva (UE) 2022/2555, prevedendo che con uno o più decreti del Presidente del Consiglio dei ministri, adottati su proposta delle competenti amministrazioni, siano esentati soggetti specifici che svolgono attività nei settori ivi indicati o che forniscono servizi esclusivamente agli enti della pubblica amministrazione di cui all'articolo 2, paragrafo 7, della medesima direttiva;

d) confermare la distinzione tra l'Agenzia per la cybersicurezza nazionale, quale autorità nazionale competente e punto di contatto, ai sensi dell'articolo 8 della direttiva (UE) 2022/2555, e le autorità di settore operanti negli ambiti di cui agli allegati I e II alla medesima direttiva;

e) in relazione all'istituzione del team di risposta agli incidenti di sicurezza informatica (CSIRT), di cui all'articolo 10 della direttiva (UE) 2022/2555, confermare le disposizioni dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65, in materia di istituzione del CSIRT Italia, nonché ampliare quanto previsto dal medesimo decreto legislativo prevedendo la collaborazione tra tutte le strutture pubbliche con funzioni di Computer Emergency Response Team (CERT) coinvolte in caso di eventi malevoli per la sicurezza informatica;

f) prevedere un regime transitorio per i soggetti già sottoposti alla disciplina del decreto legislativo 18 maggio 2018, n. 65, recante attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, garantendo termini congrui di adeguamento, ai fini della migliore applicazione delle disposizioni previste dalla direttiva (UE) 2022/2555;

g) prevedere meccanismi che consentano la registrazione dei soggetti essenziali e importanti, di cui all'articolo 3 della direttiva (UE) 2022/2555, per la comunicazione dei dati previsti dal paragrafo 4 del medesimo articolo 3, compresi i soggetti che gestiscono servizi connessi o strumentali alle attività oggetto delle disposizioni della direttiva medesima relative al settore della cultura;

h) in relazione alle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555, prevedere l'individuazione, attraverso l'utilizzo di strumenti flessibili atti a corrispondere al rapido sviluppo tecnologico, delle tecnologie necessarie ad assicurare l'effettiva attivazione delle misure stesse. L'autorità amministrativa individuata come responsabile di tale procedimento provvede altresì all'aggiornamento degli strumenti adottati;

i) introdurre nella legislazione vigente, anche in materia penale, le modifiche necessarie al fine di assicurare il corretto recepimento nell'ordinamento nazionale delle disposizioni della direttiva (UE) 2022/2555 in materia di divulgazione coordinata delle vulnerabilità;

l) definire le competenze dell'Agenzia per l'Italia digitale e dell'Agenzia per la cybersicurezza nazionale in relazione alle attività previste dal regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014;

m) individuare criteri oggettivi e proporzionati ai fini dell'applicazione degli obblighi informativi di cui all'articolo 23, paragrafo 2, della direttiva (UE) 2022/2555;

n) rivedere il sistema sanzionatorio e il sistema di vigilanza ed esecuzione, in particolare:

1) prevedendo sanzioni effettive, proporzionate e dissuasive rispetto alla gravità della violazione degli obblighi derivanti dalla direttiva (UE) 2022/2555, anche in deroga ai criteri e ai limiti previsti dall'articolo 32, comma 1, lettera *d)*, della legge 24 dicembre 2012, n. 234, e alla legge 24 novembre 1981, n. 689, introducendo strumenti deflativi del contenzioso, quali la diffida ad adempiere;

2) prevedendo che gli introiti derivanti dall'irrogazione delle sanzioni siano versati all'entrata del bilancio dello Stato per essere riassegnati all'apposito capitolo dello stato di previsione della spesa del Ministero dell'economia e delle finanze, di cui all'articolo 18 del de-

creto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, per incrementare la dotazione del bilancio dell'Agenzia per la cybersicurezza nazionale;

o) assicurare il migliore coordinamento tra le disposizioni adottate ai sensi del presente articolo per il recepimento della direttiva (UE) 2022/2555, le disposizioni adottate ai sensi dell'articolo 5 della presente legge per il recepimento della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, nonché le disposizioni del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, e quelle adottate ai sensi dell'articolo 16 della presente legge per l'adeguamento a quest'ultimo e per il recepimento della direttiva (UE) 2022/2556 del Parlamento europeo e del Consiglio, del 14 dicembre 2022;

p) apportare alla normativa vigente tutte le modificazioni e le integrazioni occorrenti ad assicurare il coordinamento con le disposizioni emanate in attuazione del presente articolo.».

— Si riporta il testo dell'articolo 8 del decreto legislativo 28 agosto 1997, n. 281 (Definizione ed ampliamento delle attribuzioni della Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e Bolzano ed unificazione, per le materie ed i compiti di interesse comune delle regioni, delle province e dei comuni, con la Conferenza Stato-città ed autonomie locali) pubblicato nella *Gazzetta Ufficiale* 30 agosto 1997, n. 202:

«Art. 8. *(Conferenza Stato-città ed autonomie locali e Conferenza unificata).* — 1. La Conferenza Stato-città ed autonomie locali è unificata per le materie ed i compiti di interesse comune delle regioni, delle province, dei comuni e delle comunità montane, con la Conferenza Stato-regioni.

2. La Conferenza Stato-città ed autonomie locali è presieduta dal Presidente del Consiglio dei Ministri o, per sua delega, dal Ministro dell'interno o dal Ministro per gli affari regionali nella materia di rispettiva competenza; ne fanno parte altresì il Ministro del tesoro e del bilancio e della programmazione economica, il Ministro delle finanze, il Ministro dei lavori pubblici, il Ministro della sanità, il presidente dell'Associazione nazionale dei comuni d'Italia - ANCI, il presidente dell'Unione province d'Italia - UPI ed il presidente dell'Unione nazionale comuni, comunità ed enti montani - UNCEM. Ne fanno parte inoltre quattordici sindaci designati dall'ANCI e sei presidenti di provincia designati dall'UPI. Dei quattordici sindaci designati dall'ANCI cinque rappresentano le città individuate dall'articolo 17 della legge 8 giugno 1990, n. 142. Alle riunioni possono essere invitati altri membri del Governo, nonché rappresentanti di amministrazioni statali, locali o di enti pubblici.

3. La Conferenza Stato-città ed autonomie locali è convocata almeno ogni tre mesi, e comunque in tutti i casi il presidente ne ravvisi la necessità o qualora ne faccia richiesta il presidente dell'ANCI, dell'UPI o dell'UNCEM.

4. La Conferenza unificata di cui al comma 1 è convocata dal Presidente del Consiglio dei Ministri. Le sedute sono presiedute dal Presidente del Consiglio dei Ministri o, su sua delega, dal Ministro per gli affari regionali o, se tale incarico non è conferito, dal Ministro dell'interno.».

Note all'art. 1:

— Si riportano gli articoli 9 e 10 del decreto-legge 14 giugno 2021, n. 82 (Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale), pubblicato nella *Gazzetta ufficiale* 14 giugno 2021, n. 140, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109 (pubblicato nella *Gazzetta Ufficiale* del 4 agosto 2021, n. 185):

«Art. 9 *(Compiti del Nucleo per la cybersicurezza).* — 1. Per le finalità di cui all'articolo 8, il Nucleo per la cybersicurezza svolge i seguenti compiti:

a) può formulare proposte di iniziative in materia di cybersicurezza del Paese, anche nel quadro del contesto internazionale in materia;

b) promuove, sulla base delle direttive di cui all'articolo 2, comma 2, la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale, in raccordo con le pianificazioni di difesa civile e di protezione civile, anche nel quadro di quanto previsto dall'articolo 7-*bis*, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198;

c) promuove e coordina lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale a esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

d) valuta e promuove, in raccordo con le amministrazioni competenti per specifici profili della cybersicurezza, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

e) acquisisce, anche per il tramite del CSIRT Italia, le comunicazioni circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi dagli organismi di informazione di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, dalle Forze di polizia e, in particolare, dall'organo del Ministero dell'interno di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, dalle strutture del Ministero della difesa, nonché dalle altre amministrazioni che compongono il Nucleo e dai gruppi di intervento per le emergenze informatiche (Computer Emergency Response Team - CERT) istituiti ai sensi della normativa vigente;

f) riceve dal CSIRT Italia le notifiche di incidente ai sensi delle disposizioni vigenti;

g) valuta se gli eventi di cui alle lettere *e)* e *f)* assumono dimensioni, intensità o natura tali da non poter essere fronteggiati dalle singole amministrazioni competenti in via ordinaria, ma richiedono l'assunzione di decisioni coordinate in sede interministeriale, provvedendo in tal caso a informare tempestivamente il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla situazione in atto e allo svolgimento delle attività di raccordo e coordinamento di cui all'articolo 10, nella composizione ivi prevista.».

«Art. 10 *(Gestione delle crisi che coinvolgono aspetti di cybersicurezza).* — 1. Nelle situazioni di crisi che coinvolgono aspetti di cybersicurezza, nei casi in cui il Presidente del Consiglio dei ministri convochi il CISR in materia di gestione delle predette situazioni di crisi, alle sedute del Comitato sono chiamati a partecipare il Ministro delegato per l'innovazione tecnologica e la transizione digitale e il direttore generale dell'Agenzia.

2.

3. In situazioni di crisi di natura cibernetica il Nucleo è integrato, in ragione della necessità, con un rappresentante, rispettivamente, del Ministero della salute e del Ministero dell'interno-Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, in rappresentanza anche della Commissione interministeriale tecnica di difesa civile, autorizzati ad assumere decisioni che impegnano la propria amministrazione. Alle riunioni i componenti possono farsi accompagnare da altri funzionari della propria amministrazione. Alle stesse riunioni possono essere chiamati a partecipare rappresentanti di altre amministrazioni, anche locali, ed enti, anche essi autorizzati ad assumere decisioni, e di altri soggetti pubblici o privati eventualmente interessati. Per la partecipazione non sono previsti compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.

4. È compito del Nucleo, nella composizione per la gestione delle crisi, di cui al comma 3, assicurare che le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti rispetto a situazioni di crisi di natura cibernetica vengano espletate in maniera coordinata secondo quanto previsto dall'articolo 9, comma 1, lettera *b).*

5. Il Nucleo, per l'espletamento delle proprie funzioni e fermo restando quanto previsto ai sensi dell'articolo 7-*bis*, comma 5, del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198:

a) mantiene costantemente informato il Presidente del Consiglio dei ministri, ovvero l'Autorità delegata, ove istituita, sulla crisi in atto, predisponendo punti aggiornati di situazione;

b) assicura il coordinamento per l'attuazione a livello interministeriale delle determinazioni del Presidente del Consiglio dei ministri per il superamento della crisi;

c) raccoglie tutti i dati relativi alla crisi;

d) elabora rapporti e fornisce informazioni sulla crisi e li trasmette ai soggetti pubblici e privati interessati;

e) partecipa ai meccanismi europei di gestione delle crisi cibernetiche, assicurando altresì i collegamenti finalizzati alla gestione della crisi con gli omologhi organismi di altri Stati, della NATO,

dell'Unione europea o di organizzazioni internazionali di cui l'Italia fa parte.».

— Per i riferimenti della direttiva (UE) 2022/2555 (misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 2:

— Si riportano gli articoli 1, come modificato dal presente decreto, nonché 5 e 8, del citato decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109:

«Art. 1 *(Definizioni)*. — 1. Ai fini del presente decreto si intende per:

a) cybersicurezza, l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico;

b) resilienza nazionale nello spazio cibernetico, le attività volte a prevenire un pregiudizio per la sicurezza nazionale come definito dall'articolo 1, comma 1, lettera *f)*, del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

c) decreto-legge perimetro, il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica;

d) *decreto legislativo NIS, il decreto legislativo di recepimento della direttiva (UE) 2022/2555, del Parlamento europeo e del Consiglio, del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148*;

e) strategia nazionale di cybersicurezza, la strategia *di cui all'articolo 9* del decreto legislativo NIS.»

«Art. 5 *(Agenzia per la cybersicurezza nazionale)*. — 1. È istituita, a tutela degli interessi nazionali nel campo della cybersicurezza, l'Agenzia per la cybersicurezza nazionale, denominata ai fini del presente decreto «Agenzia», con sede in Roma.

2. L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, nei limiti di quanto previsto dal presente decreto. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono dell'Agenzia per l'esercizio delle competenze di cui al presente decreto.

3. Il direttore generale dell'Agenzia è nominato tra soggetti appartenenti a una delle categorie di cui all'articolo 18, comma 2, della legge 23 agosto 1988, n. 400, in possesso di una documentata esperienza di elevato livello nella gestione di processi di innovazione. Gli incarichi del direttore generale e del vice direttore generale hanno la durata massima di quattro anni e sono rinnovabili, con successivi provvedimenti, per una durata complessiva massima di ulteriori quattro anni. Il direttore generale ed il vice direttore generale, ove provenienti da pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, sono collocati fuori ruolo o in posizione di comando o altra analoga posizione, secondo gli ordinamenti di appartenenza. Per quanto previsto dal presente decreto, il direttore generale dell'Agenzia è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, ed è gerarchicamente e funzionalmente sovraordinato al personale dell'Agenzia. Il direttore generale ha la rappresentanza legale dell'Agenzia.

4. L'attività dell'Agenzia è regolata dal presente decreto e dalle disposizioni la cui adozione è prevista dallo stesso.

5. L'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di precipua competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle Forze armate, delle forze di polizia o di enti pubblici per lo svolgimento dei suoi compiti istituzionali.

6. Il COPASIR, ai sensi di quanto previsto dall'articolo 31, comma 3, della legge 3 agosto 2007, n. 124, può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza.»

«Art. 8 *(Nucleo per la cybersicurezza)*. — 1. Presso l'Agenzia è costituito, in via permanente, il Nucleo per la cybersicurezza, a supporto del Presidente del Consiglio dei ministri nella materia della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento.

2. Il Nucleo per la cybersicurezza è presieduto dal direttore generale dell'Agenzia o, per sua delega, dal vice direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio dei ministri, da un rappresentante, rispettivamente, del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), di cui all'articolo 6 della legge 3 agosto 2007, n. 124, dell'Agenzia informazioni e sicurezza interna (AISI), di cui all'articolo 7 della legge n. 124 del 2007, di ciascuno dei Ministeri rappresentati nel CIC e del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri. Per gli aspetti relativi alla trattazione di informazioni classificate il Nucleo è integrato da un rappresentante dell'Ufficio centrale per la segretezza di cui all'articolo 9 della legge n. 124 del 2007.

3. I componenti del Nucleo possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione. In base agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della cybersicurezza.

4. Il Nucleo può essere convocato in composizione ristretta con la partecipazione dei rappresentanti delle sole amministrazioni e soggetti interessati, anche relativamente ai compiti di gestione delle crisi di cui all'articolo 10.

4.1. In relazione a specifiche questioni di particolare rilevanza concernenti i compiti di cui all'articolo 9, comma 1, lettera *a)*, il Nucleo può essere convocato nella composizione di cui al comma 4 del presente articolo, di volta in volta estesa alla partecipazione di un rappresentante della Direzione nazionale antimafia e antiterrorismo, della Banca d'Italia o di uno o più operatori di cui all'articolo 1, comma 2-*bis*, del decreto-legge perimetro, nonché di eventuali altri soggetti, interessati alle stesse questioni. Le amministrazioni e i soggetti convocati partecipano alle suddette riunioni a livello di vertice.

4-*bis*. Ai componenti del Nucleo non spettano compensi, gettoni di presenza, rimborsi di spese o altri emolumenti comunque denominati.».

— Per la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 si veda nelle note alle premesse.

— Per il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») si veda nelle note alle premesse.

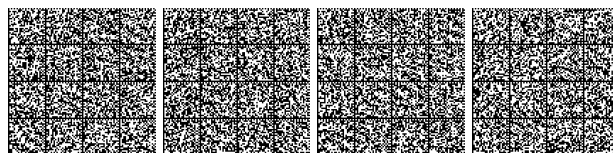
— Si riporta il testo dell'articolo 2, comma 1, lettera *vv)* del decreto legislativo 1° agosto 2003, n. 259 (Codice delle comunicazioni elettroniche) pubblicato nella *Gazzetta Ufficiale* 15 settembre 2003, n. 214

«Art. 2 *(Definizioni)*. — 1. Ai fini del presente decreto si intende per:

(*Omissis*)

vv) reti di comunicazione elettronica: i sistemi di trasmissione, basati o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa internet), i sistemi per il trasporto via cavo della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per la diffusione radiotelevisiva e le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

(*Omissis*).».

— Il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio è pubblicato nella GUUE del 14 novembre 2012 n. 316, serie L.

— La direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio del 9 settembre 2015 è pubblicata nella GUUE del 17 settembre 2015 n. 241, serie L.

— Il regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE è pubblicata nella GUUE del 28 luglio 2014 n. 257, serie L.

— La direttiva 2005/29/CE del Parlamento europeo e del Consiglio dell'11 maggio 2005 relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali») è pubblicata nella GUUE del 11 giugno 2005 n. 149, serie L.

— La direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 è pubblicata nella GUUE del 17 dicembre 2018 n. 321, serie L.

Note all'art. 3:

— La raccomandazione della Commissione del 6 maggio 2003, n. 361 è pubblicata nella GUUE del 20 maggio 2003 n. 124, serie L.

— Si riporta il testo dell'articolo 1 della legge 31 dicembre 2009, n. 196 (Legge di contabilità e finanza pubblica) pubblicata nella GU del 31 dicembre 2009, n. 303, S.O.:

«Art. 1 *(Princìpi di coordinamento e ambito di riferimento)*. — 1. Le amministrazioni pubbliche concorrono al perseguimento degli obiettivi di finanza pubblica definiti in ambito nazionale in coerenza con le procedure e i criteri stabiliti dall'Unione europea e ne condividono le conseguenti responsabilità. Il concorso al perseguimento di tali obiettivi si realizza secondo i principi fondamentali dell'armonizzazione dei bilanci pubblici e del coordinamento della finanza pubblica.

2. Ai fini della applicazione delle disposizioni in materia di finanza pubblica, per amministrazioni pubbliche si intendono, per l'anno 2011, gli enti e i soggetti indicati a fini statistici nell'elenco oggetto del comunicato dell'Istituto nazionale di statistica (ISTAT) in data 24 luglio 2010, pubblicato in pari data nella *Gazzetta Ufficiale* della Repubblica italiana n. 171, nonché a decorrere dall'anno 2012 gli enti e i soggetti indicati a fini statistici dal predetto Istituto nell'elenco oggetto del comunicato del medesimo Istituto in data 30 settembre 2011, pubblicato in pari data nella *Gazzetta Ufficiale* della Repubblica italiana n. 228, e successivi aggiornamenti ai sensi del comma 3 del presente articolo, effettuati sulla base delle definizioni di cui agli specifici regolamenti dell'Unione europea, le Autorità indipendenti e, comunque, le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni.

3. La ricognizione delle amministrazioni pubbliche di cui al comma 2 è operata annualmente dall'ISTAT con proprio provvedimento e pubblicata nella *Gazzetta Ufficiale* entro il 30 settembre.

4. Le disposizioni recate dalla presente legge e dai relativi decreti legislativi costituiscono princìpi fondamentali del coordinamento della finanza pubblica ai sensi dell'articolo 117 della Costituzione e sono finalizzate alla tutela dell'unità economica della Repubblica italiana, ai sensi dell'articolo 120, secondo comma, della Costituzione.

5. Le disposizioni della presente legge si applicano alle regioni a statuto speciale e alle province autonome di Trento e di Bolzano nel rispetto di quanto previsto dai relativi statuti».

— Si riporta, ai fini della definizione di operatore di servizi essenziali, il testo degli articoli 3 e 4 del decreto legislativo 18 maggio 2018, n. 65 (Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione) pubblicato nella GU del 9 giugno 2018, n. 132, S.O.:

«Art. 3 *(Definizioni)*. — 1. Ai fini del presente decreto si intende per:

a) autorità nazionale competente NIS, l'autorità nazionale unica, competente in materia di sicurezza delle reti e dei sistemi informativi, di cui all'articolo 7, comma 1;

a-*bis*) autorità di settore, le autorità di cui all'articolo 7, comma 1, lettere da *a)* a *e)*;

b) CSIRT, gruppo di intervento per la sicurezza informatica in caso di incidente, di cui all'articolo 8;

c) punto di contatto unico, l'organo incaricato a livello nazionale di coordinare le questioni relative alla sicurezza delle reti e dei sistemi informativi e la cooperazione transfrontaliera a livello di Unione europea;

d) autorità di contrasto, l'organo centrale del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155;

e) rete e sistema informativo:

1) una rete di comunicazione elettronica ai sensi dell'articolo 1, comma 1, lettera *dd)*, del decreto legislativo 1° agosto 2003, n. 259;

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;

f) sicurezza della rete e dei sistemi informativi, la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi;

g) operatore di servizi essenziali, soggetto pubblico o privato, della tipologia di cui all'allegato II, che soddisfa i criteri di cui all'articolo 4, comma 2;

h) servizio digitale, servizio ai sensi dell'articolo 1, paragrafo 1, lettera *b)*, della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, di un tipo elencato nell'allegato III;

i) fornitore di servizio digitale, qualsiasi persona giuridica che fornisce un servizio digitale;

l) incidente, ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi;

m) trattamento dell'incidente, tutte le procedure necessarie per l'identificazione, l'analisi e il contenimento di un incidente e l'intervento in caso di incidente;

n) rischio, ogni circostanza o evento ragionevolmente individuabile con potenziali effetti pregiudizievoli per la sicurezza della rete e dei sistemi informativi;

o) rappresentante, la persona fisica o giuridica stabilita nell'Unione europea espressamente designata ad agire per conto di un fornitore di servizi digitali che non è stabilito nell'Unione europea, a cui l'autorità competente NIS o il CSIRT Nazionale può rivolgersi in luogo del fornitore di servizi digitali, per quanto riguarda gli obblighi di quest'ultimo ai sensi del presente decreto;

p) norma, una norma ai sensi dell'articolo 2, primo paragrafo, numero 1), del regolamento (UE) n. 1025/2012;

q) specifica, una specifica tecnica ai sensi dell'articolo 2, primo paragrafo, numero 4), del regolamento (UE) n. 1025/2012;

r) punto di interscambio internet (IXP), una infrastruttura di rete che consente l'interconnessione di più di due sistemi autonomi indipendenti, principalmente al fine di agevolare lo scambio del traffico internet; un IXP fornisce interconnessione soltanto ai sistemi autonomi; un IXP non richiede che il traffico internet che passa tra qualsiasi coppia di sistemi autonomi partecipanti passi attraverso un terzo sistema autonomo, né altera o interferisce altrimenti con tale traffico;

s) sistema dei nomi di dominio (DNS), è un sistema distribuito e gerarchico di naming in una rete che inoltra le richieste dei nomi di dominio;

t) fornitore di servizi DNS, un soggetto che fornisce servizi DNS su internet;

u) registro dei nomi di dominio di primo livello, un soggetto che amministra e opera la registrazione di nomi di dominio internet nell'ambito di uno specifico dominio di primo livello (TLD);

v) mercato online, un servizio digitale che consente ai consumatori ovvero ai professionisti, come definiti rispettivamente all'articolo 141, comma 1, lettere a) e b), del decreto legislativo 6 settembre 2005, n. 206, di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato on line;

z) motore di ricerca on line, un servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto;

aa) servizio di cloud computing, un servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.»

«Art. 4 *(Identificazione degli operatori di servizi essenziali)*. — 1. Entro il 9 novembre 2018, con propri provvedimenti, le autorità competenti NIS identificano per ciascun settore e sottosettore di cui all'allegato II, gli operatori di servizi essenziali con una sede nel territorio nazionale. Gli operatori che prestano attività di assistenza sanitaria sono individuati con decreto del Ministro della salute, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano. Gli operatori che forniscono e distribuiscono acque destinate al consumo umano sono individuati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare, di intesa con la Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e di Bolzano.

2. I criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti:

a) un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;

b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi;

c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

3. Oltre ai criteri indicati nel comma 2, nell'individuazione degli operatori di servizi essenziali si tiene conto dei documenti prodotti al riguardo dal Gruppo di cooperazione di cui all'articolo 10.

4. Ai fini del comma 1, prima dell'adozione dei provvedimenti previsti dalla medesima disposizione, qualora un soggetto fornisca un servizio di cui al comma 2, lettera *a)*, sul territorio nazionale e in altro o altri Stati membri dell'Unione europea, le autorità competenti NIS consultano le autorità competenti degli altri Stati membri.

5. È istituito presso il Ministero dello sviluppo economico un elenco nazionale degli operatori di servizi essenziali. Il Ministero dello sviluppo economico inoltra tale elenco al punto di contatto unico e all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

6. L'elenco degli operatori di servizi essenziali identificati ai sensi del comma 1 è riesaminato e, se del caso, aggiornato su base regolare, e almeno ogni due anni dopo il 9 maggio 2018, con le seguenti modalità:

a) le autorità di settore, in relazione ai settori di competenza, propongono all'autorità nazionale competente NIS le variazioni all'elenco degli operatori dei servizi essenziali, secondo i criteri di cui ai commi 2 e 3;

b) le proposte sono valutate ed eventualmente integrate, d'intesa con le autorità di settore, dall'autorità nazionale competente NIS che, con propri provvedimenti, provvede alle variazioni dell'elenco degli operatori dei servizi essenziali, dandone comunicazione, in relazione ai settori di competenza, anche alle autorità di settore.

7. Entro il 9 novembre 2018, e in seguito ogni due anni, il punto di contatto unico trasmette alla Commissione europea le informazioni necessarie per la valutazione dell'attuazione del presente decreto, in particolare della coerenza dell'approccio in merito all'identificazione degli operatori di servizi essenziali.

8. Le informazioni di cui al comma 7 comprendono almeno:

a) le misure nazionali che consentono l'identificazione degli operatori di servizi essenziali;

b) l'elenco dei servizi di cui al comma 2;

c) il numero degli operatori di servizi essenziali identificati per ciascun settore di cui all'allegato II ed un'indicazione della loro importanza in relazione a tale settore;

d) le soglie, ove esistano, per determinare il pertinente livello di fornitura con riferimento al numero di utenti che dipendono da tale servizio di cui all'articolo 5, comma 1, lettera *a)*, o all'importanza di tale particolare operatore di servizi essenziali di cui all'articolo 5, comma 1, lettera *f)*.».

Note all'art. 4:

— Si riporta il testo dell'articolo 6 del decreto legislativo 21 novembre 2007, n. 231 (Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione) pubblicato nella GU del 14 dicembre 2007, n. 290, S.O.:

«Art. 6 *(Unità d'informazione finanziaria)*. — 1. L'Unità di informazione finanziaria per l'Italia (UIF), istituita presso la Banca d'Italia, è autonoma e operativamente indipendente. In attuazione di tale principio, la Banca d'Italia ne disciplina con regolamento l'organizzazione e il funzionamento, ivi compresa la riservatezza delle informazioni acquisite, attribuendole i mezzi finanziari e le risorse idonei ad assicurare l'efficace perseguimento dei suoi fini istituzionali. Alla UIF e al personale addetto si applica l'articolo 24, comma 6-*bis*, della legge 28 dicembre 2005, n. 262. (41)

2. Il Direttore della UIF, al quale compete in autonomia la responsabilità della gestione, è nominato con provvedimento del Direttorio della Banca d'Italia, su proposta del Governatore della Banca d'Italia, tra persone dotate di adeguati requisiti di onorabilità, professionalità e conoscenza del sistema finanziario. Il mandato ha la durata di cinque anni ed è rinnovabile una sola volta.

3. Per l'efficace svolgimento dei compiti fissati dalla legge e dagli obblighi internazionali, presso la UIF è costituito un Comitato di esperti, del quale fanno parte il Direttore e quattro membri, dotati di adeguati requisiti di onorabilità e professionalità. I componenti del Comitato sono nominati, nel rispetto del principio dell'equilibrio di genere, con decreto del Ministro dell'economia e delle finanze, sentito il Governatore della Banca d'Italia, e restano in carica tre anni, rinnovabili per altri tre. La partecipazione al Comitato non dà luogo a compensi. Il Comitato è convocato dal Direttore della UIF con cadenza almeno semestrale e svolge funzioni di consulenza e ausilio a supporto dell'azione della UIF. Il Comitato cura, altresì, la redazione di un parere sull'azione dell'UIF, che forma parte integrante della documentazione trasmessa al Parlamento ai sensi del comma 8.

4. La UIF esercita le seguenti funzioni:

a) riceve le segnalazioni di operazioni sospette e ne effettua l'analisi finanziaria;

b) analizza i flussi finanziari, al fine di individuare e prevenire fenomeni di riciclaggio di denaro e di finanziamento del terrorismo;

c) può sospendere, per un massimo di cinque giorni lavorativi, operazioni sospette, anche su richiesta del Nucleo speciale di polizia valutaria della Guardia di finanza, della Direzione investigativa antimafia e dell'autorità giudiziaria ovvero su richiesta di un'altra FIU, ove non ne derivi pregiudizio per il corso delle indagini. La UIF provvede a dare immediata notizia della sospensione all'autorità che ne ha fatto richiesta;

d) avuto riguardo alle caratteristiche dei soggetti obbligati, emana istruzioni, pubblicate nella *Gazzetta Ufficiale* della Repubblica italiana, sui dati e le informazioni che devono essere contenuti nelle segnalazioni di operazioni sospette e nelle comunicazioni oggettive, sulla relativa tempistica nonché sulle modalità di tutela della riservatezza dell'identità del segnalante;

e) al fine di agevolare l'individuazione delle operazioni sospette, emana e aggiorna periodicamente, previa presentazione al Comitato di sicurezza finanziaria, indicatori di anomalia, pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana e in apposita sezione del proprio sito istituzionale;

f) effettua, anche attraverso ispezioni, verifiche al fine di accertare il rispetto delle disposizioni in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, con riguardo alle segnalazioni di operazioni sospette e ai casi di omessa segnalazione di operazioni sospette, nonché con riguardo alle comunicazioni alla UIF previste dal presente decreto e ai casi di omissione delle medesime, anche avvalendosi della collaborazione del Nucleo speciale di polizia valutaria della Guardia di finanza;

g) in relazione ai propri compiti, accerta e contesta ovvero trasmette alle autorità di vigilanza di settore le violazioni degli obblighi di cui al presente decreto di cui viene a conoscenza nell'esercizio delle proprie funzioni istituzionali;

h) assicura la tempestiva trasmissione alla Direzione nazionale antimafia e antiterrorismo dei dati, delle informazioni e delle analisi, secondo quanto stabilito dall'articolo 8, comma 1, lettera *a)*. Assicura, altresì, l'effettuazione delle analisi richieste dalla Direzione nazionale antimafia e antiterrorismo ai sensi dell'articolo 8, comma 1, lettera *d)*.

5. Per lo svolgimento delle proprie funzioni istituzionali, la UIF:

a) acquisisce, anche attraverso ispezioni, dati e informazioni presso i soggetti destinatari degli obblighi di cui al presente decreto;

b) riceve la comunicazione dei dati statistici aggregati da parte dei soggetti obbligati tenuti a effettuarla e le comunicazioni cui sono tenute le Pubbliche amministrazioni, ai sensi dell'articolo 10.

6. Per l'esercizio delle funzioni di cui ai commi 4 e 5, la UIF:

a) si avvale dei dati contenuti nell'anagrafe dei conti e dei depositi di cui all'articolo 20, comma 4, della legge 30 dicembre 1991, n. 413, e nell'anagrafe tributaria di cui all'articolo 37 del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248;

b) ha accesso ai dati e alle informazioni contenute nell'anagrafe immobiliare integrata di cui all'articolo 19 del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni dalla legge 30 luglio 2010, n. 122;

c) ha accesso alle informazioni sul titolare effettivo di persone giuridiche e trust espressi, contenute in apposita sezione del Registro delle imprese, ai sensi dell'articolo 21 del presente decreto.

7. Avvalendosi delle informazioni raccolte nello svolgimento delle proprie funzioni, la UIF:

a) svolge analisi e studi su singole anomalie, riferibili a ipotesi di riciclaggio e di finanziamento del terrorismo su specifici settori dell'economia ritenuti a rischio, su categorie di strumenti di pagamento e su specifiche realtà economiche territoriali, anche sulla base dell'analisi nazionale dei rischi elaborata dal Comitato di sicurezza finanziaria;

b) elabora e diffonde modelli e schemi rappresentativi di comportamenti anomali sul piano economico e finanziario riferibili a possibili attività di riciclaggio e di finanziamento del terrorismo.

8. Ai fini della presentazione al Parlamento della relazione sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, il Direttore della UIF, entro il 30 maggio di ogni anno, trasmette al Ministro dell'economia e delle finanze, per il tramite del Comitato di sicurezza finanziaria, gli allegati alla medesima relazione, di cui all'articolo 4, comma 2, del presente decreto.».

— Si riporta il testo degli articoli 4, 6, 7 e 43 della legge 3 agosto 2007, n. 124 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto) pubblicata nella GU del 13 agosto 2007, n. 187:

«Art. 4 *(Dipartimento delle informazioni per la sicurezza)*. — 1. Per lo svolgimento dei compiti di cui al comma 3 è istituito, presso la Presidenza del Consiglio dei ministri, il Dipartimento delle informazioni per la sicurezza (DIS).

2. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono del DIS per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza, nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza.

3. Il DIS svolge i seguenti compiti:

a) coordina l'intera attività di informazione per la sicurezza, verificando altresì i risultati delle attività svolte dall'AISE e dall'AISI, ferma restando la competenza dei predetti servizi relativamente alle attività di ricerca informativa e di collaborazione con i servizi di sicurezza degli Stati esteri;

b) è costantemente informato delle operazioni di competenza dei servizi di informazione per la sicurezza e trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte dal Sistema di informazione per la sicurezza;

c) raccoglie le informazioni, le analisi e i rapporti provenienti dai servizi di informazione per la sicurezza, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati; ferma l'esclusiva competenza dell'AISE e dell'AISI per l'elaborazione dei rispettivi piani di ricerca operativa, elabora analisi strategiche o relative a particolari situazioni; formula valutazioni e previsioni, sulla scorta dei contributi analitici settoriali dell'AISE e dell'AISI;

d) elabora, anche sulla base delle informazioni e dei rapporti di cui alla lettera *c)*, analisi globali da sottoporre al CISR, nonché progetti di ricerca informativa, sui quali decide il Presidente del Consiglio dei ministri, dopo avere acquisito il parere del CISR;

d-*bis*) sulla base delle direttive di cui all'articolo 1, comma 3-*bis*, nonché delle informazioni e dei rapporti di cui alla lettera *c)* del presente comma, coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

e) promuove e garantisce, anche attraverso riunioni periodiche, lo scambio informativo tra l'AISE, l'AISI e le Forze di polizia; comunica al Presidente del Consiglio dei ministri le acquisizioni provenienti dallo scambio informativo e i risultati delle riunioni periodiche;

f) trasmette, su disposizione del Presidente del Consiglio dei ministri, sentito il CISR, informazioni e analisi ad amministrazioni pubbliche o enti, anche ad ordinamento autonomo, interessati all'acquisizione di informazioni per la sicurezza;

g) elabora, d'intesa con l'AISE e l'AISI, il piano di acquisizione delle risorse umane e materiali e di ogni altra risorsa comunque strumentale all'attività dei servizi di informazione per la sicurezza, da sottoporre all'approvazione del Presidente del Consiglio dei ministri;

h) sentite l'AISE e l'AISI, elabora e sottopone all'approvazione del Presidente del Consiglio dei ministri lo schema del regolamento di cui all'articolo 21, comma 1;

i) esercita il controllo sull'AISE e sull'AISI, verificando la conformità delle attività di informazione per la sicurezza alle leggi e ai regolamenti, nonché alle direttive e alle disposizioni del Presidente del Consiglio dei ministri. Per tale finalità, presso il DIS è istituito un ufficio ispettivo le cui modalità di organizzazione e di funzionamento sono definite con il regolamento di cui al comma 7. Con le modalità previste da tale regolamento è approvato annualmente, previo parere del Comitato parlamentare di cui all'articolo 30, il piano annuale delle attività dell'ufficio ispettivo. L'ufficio ispettivo, nell'ambito delle competenze definite con il predetto regolamento, può svolgere, anche a richiesta del direttore generale del DIS, autorizzato dal Presidente del Consiglio dei ministri, inchieste interne su specifici episodi e comportamenti verificatisi nell'ambito dei servizi di informazione per la sicurezza;

l) assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei Ministri con apposito regolamento adottato ai sensi dell'articolo 1, comma 2, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione;

m) cura le attività di promozione e diffusione della cultura della sicurezza e la comunicazione istituzionale;

n) impartisce gli indirizzi per la gestione unitaria del personale di cui all'articolo 21, secondo le modalità definite dal regolamento di cui al comma 1 del medesimo articolo;

n-*bis*) gestisce unitariamente, ferme restando le competenze operative dell'AISE e dell'AISI, gli approvvigionamenti e i servizi logistici comuni.

4. Fermo restando quanto previsto dall'articolo 118-*bis* del codice di procedura penale, introdotto dall'articolo 14 della presente legge, qualora le informazioni richieste alle Forze di polizia, ai sensi delle lettere *c)* ed *e)* del comma 3 del presente articolo, siano relative a indagini di polizia giudiziaria, le stesse, se coperte dal segreto di cui all'articolo 329 del codice di procedura penale, possono essere acquisite solo previo nulla osta della autorità giudiziaria competente. L'autorità giudiziaria può trasmettere gli atti e le informazioni anche di propria iniziativa.

5. La direzione generale del DIS è affidata ad un dirigente di prima fascia o equiparato dell'amministrazione dello Stato, la cui nomina e revoca spettano in via esclusiva al Presidente del Consiglio dei ministri, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio. Per quanto previsto dalla presente legge, il direttore del DIS è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, salvo quanto previsto dall'articolo 6, comma 5, e dall'articolo 7, comma 5, ed è gerarchicamente e funzionalmente sovraordinato al personale del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento.

6. Il Presidente del Consiglio dei ministri, sentito il direttore generale del DIS, nomina uno o più vice direttori generali; il direttore generale affida gli altri incarichi nell'ambito del Dipartimento, ad eccezione degli incarichi il cui conferimento spetta al Presidente del Consiglio dei ministri.

7. L'ordinamento e l'organizzazione del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento sono disciplinati con apposito regolamento.

8. Il regolamento previsto dal comma 7 definisce le modalità di organizzazione e di funzionamento dell'ufficio ispettivo di cui al comma 3, lettera *i)*, secondo i seguenti criteri:

a) agli ispettori è garantita piena autonomia e indipendenza di giudizio nell'esercizio delle funzioni di controllo;

b) salva specifica autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, i controlli non devono interferire con le operazioni in corso;

c) sono previste per gli ispettori specifiche prove selettive e un'adeguata formazione;

d) non è consentito il passaggio di personale dall'ufficio ispettivo ai servizi di informazione per la sicurezza;

e) gli ispettori, previa autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, possono accedere a tutti gli atti conservati presso i servizi di informazione per la sicurezza e presso il DIS; possono altresì acquisire, tramite il direttore generale del DIS, altre informazioni da enti pubblici e privati.»

«Art. 6 *(Agenzia informazioni e sicurezza esterna)*. — 1. È istituita l'Agenzia informazioni e sicurezza esterna (AISE), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica, anche in attuazione di accordi internazionali, dalle minacce provenienti dall'estero.

2. Spettano all'AISE inoltre le attività in materia di controproliferazione concernenti i materiali strategici, nonché le attività di informazione per la sicurezza, che si svolgono al di fuori del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISE individuare e contrastare al di fuori del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISE può svolgere operazioni sul territorio nazionale soltanto in collaborazione con l'AISI, quando tali operazioni siano strettamente connesse ad attività che la stessa AISE svolge all'estero. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISE risponde al Presidente del Consiglio dei ministri.

6. L'AISE informa tempestivamente e con continuità il Ministro della difesa, il Ministro degli affari esteri e il Ministro dell'interno per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri, con proprio decreto, nomina e revoca il direttore dell'AISE, scelto tra dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

8. Il direttore dell'AISE riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISE, uno o più vice direttori. Il direttore dell'AISE affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISE sono disciplinati con apposito regolamento.»

«Art. 7 *(Agenzia informazioni e sicurezza interna)*. — 1. È istituita l'Agenzia informazioni e sicurezza interna (AISI), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili a difendere, anche in attuazione di accordi internazionali, la sicurezza interna della Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica.

2. Spettano all'AISI le attività di informazione per la sicurezza, che si svolgono all'interno del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISI individuare e contrastare all'interno del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISI può svolgere operazioni all'estero soltanto in collaborazione con l'AISE, quando tali operazioni siano strettamente connesse ad attività che la stessa AISI svolge all'interno del territorio nazionale. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISI risponde al Presidente del Consiglio dei ministri.

6. L'AISI informa tempestivamente e con continuità il Ministro dell'interno, il Ministro degli affari esteri e il Ministro della difesa per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri nomina e revoca, con proprio decreto, il direttore dell'AISI, scelto tra i dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

8. Il direttore dell'AISI riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISI, uno o più vice direttori. Il direttore dell'AISI affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISI sono disciplinati con apposito regolamento.»

«Art. 43 *(Procedura per l'adozione dei regolamenti)*. — 1. Salvo che non sia diversamente stabilito, le disposizioni regolamentari previste dalla presente legge sono emanate entro centottanta giorni dalla data della sua entrata in vigore, con uno o più decreti del Presidente del Consiglio dei ministri adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e successive modificazioni, previo parere del Comitato parlamentare di cui all'articolo 30 e sentito il CISR.

2. I suddetti decreti stabiliscono il regime della loro pubblicità, anche in deroga alle norme vigenti.».

— Il Trattato sul funzionamento dell'Unione Europea (versione vigente) è pubblicato nella GUUE del 26 ottobre 2012 n. 326 serie C.

Note all'art. 6:

— Per i riferimenti della raccomandazione della Commissione del 6 maggio 2003, n. 361, si veda nelle note all'art. 3.

«Art. 2 *(Effettivi e soglie finanziarie che definiscono le categorie di imprese)*. — 1. La categoria delle microimprese delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di EUR oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR.

2. Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di 50 persone e realizza un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di EUR.

3. Nella categoria delle PMI si definisce microimpresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR.».

Note all'art. 8:

— Il testo del decreto legislativo 30 giugno 2003, n. 196 recante «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» è pubblicato nella *Gazzetta ufficiale* del 29 luglio 2003, n. 174, S.O..

— Per i riferimenti alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio dei 12 luglio 2022 (Direttiva relativa alla vita privata e alle comunicazioni elettroniche) si veda nelle note alle premesse

Note all'art. 9:

— Per i riferimenti alla direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, si veda nelle note alle premesse.

— Si riporta il testo dell'articolo 2, del citato decreto-legge 14 giugno 2021, n. 82.

«Art. 2 *(Competenze del Presidente del Consiglio dei ministri)*. — 1. Al Presidente del Consiglio dei ministri sono attribuite in via esclusiva:

a) l'alta direzione e la responsabilità generale delle politiche di cybersicurezza;

b) l'adozione della strategia nazionale di cybersicurezza, sentito il Comitato interministeriale per la cybersicurezza (CIC) di cui all'articolo 4;

c) la nomina e la revoca del direttore generale e del vice direttore generale dell'Agenzia per la cybersicurezza nazionale di cui all'articolo 5, previa deliberazione del Consiglio dei ministri.

2. Ai fini dell'esercizio delle competenze di cui al comma 1, lettera *a)*, e dell'attuazione della strategia nazionale di cybersicurezza, il Presidente del Consiglio dei ministri, sentito il CIC, impartisce le direttive per la cybersicurezza ed emana ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia per la cybersicurezza nazionale.

3. Il Presidente del Consiglio dei ministri informa preventivamente il Comitato parlamentare per la sicurezza della Repubblica (COPASIR), di cui all'articolo 30 della legge 3 agosto 2007, n. 124, e le Commissioni parlamentari competenti circa le nomine di cui al comma 1, lettera *c)*, del presente articolo».

— Si riporta il testo dell'articolo 7 del citato decreto-legge 14 giugno 2021, n. 82:

«Art. 7 *(Funzioni dell'Agenzia per la cybersicurezza nazionale)*. — 1. L'Agenzia:

a) è Autorità nazionale per la cybersicurezza e, in relazione a tale ruolo, assicura, nel rispetto delle competenze attribuite dalla normativa vigente ad altre amministrazioni, ferme restando le attribuzioni del Ministro dell'interno in qualità di autorità nazionale di pubblica sicurezza, ai sensi della legge 1° aprile 1981, n. 121, il coordinamento tra i soggetti pubblici coinvolti in materia di cybersicurezza a livello nazionale e promuove la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni, nonché per il conseguimento dell'autonomia, nazionale ed europea, riguardo a prodotti e processi informatici di rilevanza strategica a tutela degli interessi nazionali nel settore. Per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate restano fermi sia quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge n. 124 del 2007, sia le competenze dell'Ufficio centrale per la segretezza di cui all'articolo 9 della medesima legge n. 124 del 2007;

b) predispone la strategia nazionale di cybersicurezza;

c) svolge ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza, di cui all'articolo 8;

d) è Autorità nazionale competente e punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi, per le finalità di cui al decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento, ed è competente all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto;

e) è Autorità nazionale di certificazione della cybersicurezza ai sensi dell'articolo 58 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, e assume tutte le funzioni in materia di certificazione di sicurezza cibernetica già attribuite al Ministero dello sviluppo economico dall'ordinamento vigente, comprese quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni; nello svolgimento dei compiti di cui alla presente lettera:

1) accredita, ai sensi dell'articolo 60, paragrafo 1, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, le strutture specializzate del Ministero della difesa e del Ministero dell'interno quali organismi di valutazione della conformità per i sistemi di rispettiva competenza;

2) delega, ai sensi dell'articolo 56, paragrafo 6, lettera *b)*, del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, il Ministero della difesa e il Ministero dell'interno, attraverso le rispettive strutture accreditate di cui al numero 1) della presente lettera, al rilascio del certificato europeo di sicurezza cibernetica;

f) assume tutte le funzioni in materia di cybersicurezza già attribuite dalle disposizioni vigenti al Ministero dello sviluppo economico, ivi comprese quelle relative:

1) al perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le funzioni attribuite al Centro di valutazione e certificazione nazionale ai sensi del decreto-legge perimetro, le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131;

2) alla sicurezza e all'integrità delle comunicazioni elettroniche, di cui agli articoli 16-*bis* e 16-*ter* del decreto legislativo 1° agosto 2003, n. 259, e relative disposizioni attuative;

3) alla sicurezza delle reti e dei sistemi informativi, di cui al decreto legislativo NIS;

g) partecipa, per gli ambiti di competenza, al gruppo di coordinamento istituito ai sensi dei regolamenti di cui all'articolo 1, comma 8, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56;

h) assume tutte le funzioni attribuite alla Presidenza del Consiglio dei ministri in materia di perimetro di sicurezza nazionale cibernetica, di cui al decreto-legge perimetro e ai relativi provvedimenti attuativi, ivi incluse le attività di ispezione e verifica di cui all'articolo 1, comma 6, lettera *c)*, del decreto-legge perimetro e quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative previste dal medesimo decreto, fatte salve quelle di cui all'articolo 3 del regolamento adottato con decreto del Presidente del Consiglio dei ministri n. 131 del 2020;

i) assume tutte le funzioni già attribuite al Dipartimento delle informazioni per la sicurezza (DIS), di cui all'articolo 4 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi e supporta il Presidente del Consiglio dei ministri ai fini dell'articolo 1, comma 19-*bis*, del decreto-legge perimetro;

l) provvede, sulla base delle attività di competenza del Nucleo per la cybersicurezza di cui all'articolo 8, alle attività necessarie per l'attuazione e il controllo dell'esecuzione dei provvedimenti assunti dal Presidente del Consiglio dei ministri ai sensi dell'articolo 5 del decreto-legge perimetro;

m) assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché quelle in materia di adozione di linee guida contenenti regole tecniche di cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale;

m-*bis*) provvede, anche attraverso un'apposita sezione nell'ambito della strategia di cui alla lettera *b)*, allo sviluppo e alla diffusione di standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici, alla valutazione della sicurezza dei sistemi crittografici nonché all'organizzazione e alla gestione di attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia, anche a vantaggio della tecnologia blockchain, come strumento di cybersicurezza. L'Agenzia, anche per il rafforzamento dell'autonomia industriale e tecnologica dell'Italia, promuove altresì la collaborazione con centri universitari e di ricerca per la valorizzazione dello sviluppo di nuovi algoritmi proprietari, la ricerca e il conseguimento di nuove capacità crittografiche nazionali nonché la collaborazione internazionale con gli organismi esteri che svolgono analoghe funzioni. A tale fine, è istituito presso l'Agenzia, nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e senza nuovi o maggiori oneri a carico della finanza pubblica, il Centro nazionale di crittografia, il cui funzionamento è disciplinato con provvedimento del direttore generale dell'Agenzia stessa. Il Centro nazionale di crittografia svolge le funzioni di centro di competenza nazionale per tutti gli aspetti della crittografia in ambito non classificato, ferme restando le competenze dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge

3 agosto 2007, n. 124, con riferimento alle informazioni e alle attività previste dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della citata legge n. 124 del 2007, nonché le competenze degli organismi di cui agli articoli 4, 6 e 7 della medesima legge;

m-*ter*) provvede alla qualificazione dei servizi cloud per la pubblica amministrazione nel rispetto della disciplina dell'Unione europea e del regolamento di cui all'articolo 33-*septies*, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221;

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il CSIRT Italia di cui all'articolo 8 del decreto legislativo NIS. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;

n-*bis*) nell'ambito delle funzioni di cui al primo periodo della lettera *n)*, svolge ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subìto incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge perimetro, di cui all'articolo 3, comma 1, lettere *g)* e *i)*, del decreto legislativo NIS e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;

n-*ter*) provvede alla raccolta, all'elaborazione e alla classificazione dei dati relativi alle notifiche di incidenti ricevute dai soggetti che a ciò siano tenuti in osservanza delle disposizioni vigenti. Tali dati sono resi pubblici nell'ambito della relazione prevista dall'articolo 14, comma 1, quali dati ufficiali di riferimento degli attacchi informatici portati ai soggetti che operano nei settori rilevanti per gli interessi nazionali nel campo della cybersicurezza. Agli adempimenti previsti dalla presente lettera si provvede con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente;

o) partecipa alle esercitazioni nazionali e internazionali che riguardano la simulazione di eventi di natura cibernetica al fine di innalzare la resilienza del Paese;

p) cura e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale. A tal fine, l'Agenzia esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza;

q) coordina, in raccordo con il Ministero degli affari esteri e della cooperazione internazionale, la cooperazione internazionale nella materia della cybersicurezza. Nell'ambito dell'Unione europea e a livello internazionale, l'Agenzia cura i rapporti con i competenti organismi, istituzioni ed enti, nonché segue nelle competenti sedi istituzionali le tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni. In tali casi, è comunque assicurato il raccordo con l'Agenzia al fine di garantire posizioni nazionali unitarie e coerenti con le politiche di cybersicurezza definite dal Presidente del Consiglio dei ministri;

r) perseguendo obiettivi di eccellenza, supporta negli ambiti di competenza, mediante il coinvolgimento del sistema dell'università e della ricerca nonché del sistema produttivo nazionali, lo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche. A tali fini, l'Agenzia può promuovere, sviluppare e finanziare specifici progetti ed iniziative, volti anche a favorire il trasferimento tecnologico dei risultati della ricerca nel settore. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti alla ricerca militare. L'Agenzia può altresì promuovere la costituzione di aree dedicate allo sviluppo dell'innovazione finalizzate a favorire la formazione e il reclutamento di personale nei settori avanzati dello sviluppo della cybersicurezza, nonché promuovere la realizzazione di studi di fattibilità e di analisi valutative finalizzati a tale scopo;

s) stipula accordi bilaterali e multilaterali, anche mediante il coinvolgimento del settore privato e industriale, con istituzioni, enti e organismi di altri Paesi per la partecipazione dell'Italia a programmi di cybersicurezza, assicurando il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale;

t) promuove, sostiene e coordina la partecipazione italiana a progetti e iniziative dell'Unione europea e internazionali, anche mediante il coinvolgimento di soggetti pubblici e privati nazionali, nel campo della cybersicurezza e dei correlati servizi applicativi, ferme restando le competenze del Ministero degli affari esteri e della cooperazione internazionale. L'Agenzia assicura il necessario raccordo con le altre amministrazioni a cui la legge attribuisce competenze in materia di cybersicurezza e, in particolare, con il Ministero della difesa per gli aspetti inerenti a progetti e iniziative in collaborazione con la NATO e con l'Agenzia europea per la difesa;

u) svolge attività di comunicazione e promozione della consapevolezza in materia di cybersicurezza, al fine di contribuire allo sviluppo di una cultura nazionale in materia;

v) promuove la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati; nello svolgimento di tali compiti, l'Agenzia può avvalersi anche delle strutture formative e delle capacità della Presidenza del Consiglio dei ministri, del Ministero della difesa e del Ministero dell'interno, secondo termini e modalità da definire con apposito decreto del Presidente del Consiglio dei ministri, di concerto con i Ministri interessati;

v-*bis*) può predisporre attività di formazione specifica riservate ai giovani che aderiscono al servizio civile regolate sulla base di apposite convenzioni. In ogni caso, il servizio prestato è, a tutti gli effetti, riconosciuto come servizio civile;

z) per le finalità di cui al presente articolo, può costituire e partecipare a partenariati pubblico-privato sul territorio nazionale, nonché, previa autorizzazione del Presidente del Consiglio dei ministri, a consorzi, fondazioni o società con soggetti pubblici e privati, italiani e stranieri;

aa) è designata quale Centro nazionale di coordinamento ai sensi dell'articolo 6 del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

1-*bis*. Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere *r)*, *s)*, *t)*, *u)*, *v)*, *z)* e *aa)*, presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1. Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.

3. Il CSIRT italiano di cui all'articolo 8 del decreto legislativo NIS è trasferito presso l'Agenzia e assume la denominazione di: "CSIRT Italia".

4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.

5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili

a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.».

Note all'art. 10:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 11:

— Si riporta il testo dell'articolo 30 del decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche):

«Art. 30 *(Passaggio diretto di personale tra amministrazioni diverse)*. — 1. Le amministrazioni possono ricoprire posti vacanti in organico mediante passaggio diretto di dipendenti di cui all'articolo 2, comma 2, appartenenti a una qualifica corrispondente e in servizio presso altre amministrazioni, che facciano domanda di trasferimento. È richiesto il previo assenso dell'amministrazione di appartenenza nel caso in cui si tratti di posizioni dichiarate motivatamente infungibili dall'amministrazione cedente o di personale assunto da meno di tre anni o qualora la mobilità determini una carenza di organico superiore al 20 per cento nella qualifica corrispondente a quella del richiedente. È fatta salva la possibilità di differire, per motivate esigenze organizzative, il passaggio diretto del dipendente fino ad un massimo di sessanta giorni dalla ricezione dell'istanza di passaggio diretto ad altra amministrazione. Le disposizioni di cui ai periodi secondo e terzo non si applicano al personale delle aziende e degli enti del servizio sanitario nazionale e degli enti locali con un numero di dipendenti a tempo indeterminato non superiore a 100, per i quali è comunque richiesto il previo assenso dell'amministrazione di appartenenza. Al personale della scuola continuano ad applicarsi le disposizioni vigenti in materia. Le amministrazioni, fissando preventivamente i requisiti e le competenze professionali richieste, pubblicano sul proprio sito istituzionale, per un periodo pari almeno a trenta giorni, un bando in cui sono indicati i posti che intendono ricoprire attraverso passaggio diretto di personale di altre amministrazioni, con indicazione dei requisiti da possedere. In via sperimentale e fino all'introduzione di nuove procedure per la determinazione dei fabbisogni standard di personale delle amministrazioni pubbliche, per il trasferimento tra le sedi centrali di differenti ministeri, agenzie ed enti pubblici non economici nazionali non è richiesto l'assenso dell'amministrazione di appartenenza, la quale dispone il trasferimento entro due mesi dalla richiesta dell'amministrazione di destinazione, fatti salvi i termini per il preavviso e a condizione che l'amministrazione di destinazione abbia una percentuale di posti vacanti superiore all'amministrazione di appartenenza.

1.1. Per gli enti locali con un numero di dipendenti compreso tra 101 e 250, la percentuale di cui al comma 1 è stabilita al 5 per cento; per gli enti locali con un numero di dipendenti non superiore a 500, la predetta percentuale è fissata al 10 per cento. La percentuale di cui al comma 1 è da considerare all'esito della mobilità e riferita alla dotazione organica dell'ente.

1-*bis*. L'amministrazione di destinazione provvede alla riqualificazione dei dipendenti la cui domanda di trasferimento è accolta, eventualmente avvalendosi, ove sia necessario predisporre percorsi specifici o settoriali di formazione, della Scuola nazionale dell'amministrazione. All'attuazione del presente comma si provvede utilizzando le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri per la finanza pubblica.

1-*ter*. La dipendente vittima di violenza di genere inserita in specifici percorsi di protezione, debitamente certificati dai servizi sociali del comune di residenza, può presentare domanda di trasferimento ad altra amministrazione pubblica ubicata in un comune diverso da quello di residenza, previa comunicazione all'amministrazione di appartenenza. Entro quindici giorni dalla suddetta comunicazione l'amministrazione di appartenenza dispone il trasferimento presso l'amministrazione indicata dalla dipendente, ove vi siano posti vacanti corrispondenti alla sua qualifica professionale.

1-*quater*. A decorrere dal 1° luglio 2022, ai fini di cui al comma 1 e in ogni caso di avvio di procedure di mobilità, le amministrazioni provvedono a pubblicare il relativo avviso in una apposita sezione del Portale unico del reclutamento di cui all'articolo 35-*ter*. Il personale interessato a partecipare alle predette procedure invia la propria candidatura, per qualsiasi posizione disponibile, previa registrazione nel Portale corredata del proprio curriculum vitae esclusivamente in formato digitale. Dalla presente disposizione non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

1-*quinquies*. Per il personale non dirigenziale delle amministrazioni di cui all'articolo 1, comma 2, delle autorità amministrative indipendenti e dei soggetti di cui all'articolo 70, comma 4, i comandi o distacchi sono consentiti esclusivamente nel limite del 25 per cento dei posti non coperti all'esito delle procedure di mobilità di cui al presente articolo. La disposizione di cui al primo periodo non si applica ai comandi o distacchi obbligatori, previsti da disposizioni di legge, ivi inclusi quelli relativi agli uffici di diretta collaborazione, nonché a quelli relativi alla partecipazione ad organi, comunque denominati, istituiti da disposizioni legislative o regolamentari che prevedono la partecipazione di personale di amministrazioni diverse, nonché ai comandi presso le sedi territoriali dei ministeri, o presso le Unioni di comuni per i Comuni che ne fanno parte.

2. Nell'ambito dei rapporti di lavoro di cui all'articolo 2, comma 2, i dipendenti possono essere trasferiti all'interno della stessa amministrazione o, previo accordo tra le amministrazioni interessate, in altra amministrazione, in sedi collocate nel territorio dello stesso comune ovvero a distanza non superiore a cinquanta chilometri dalla sede cui sono adibiti. Ai fini del presente comma non si applica il terzo periodo del primo comma dell'articolo 2103 del codice civile. Con decreto del Ministro per la semplificazione e la pubblica amministrazione, previa consultazione con le confederazioni sindacali rappresentative e previa intesa, ove necessario, in sede di conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, possono essere fissati criteri per realizzare i processi di cui al presente comma, anche con passaggi diretti di personale tra amministrazioni senza preventivo accordo, per garantire l'esercizio delle funzioni istituzionali da parte delle amministrazioni che presentano carenze di organico. Le disposizioni di cui al presente comma si applicano ai dipendenti con figli di età inferiore a tre anni, che hanno diritto al congedo parentale, e ai soggetti di cui all'articolo 33, comma 3, della legge 5 febbraio 1992, n. 104, e successive modificazioni, con il consenso degli stessi alla prestazione della propria attività lavorativa in un'altra sede.

2.1. Nei casi di cui ai commi 1 e 2 per i quali sia necessario un trasferimento di risorse, si applica il comma 2.3.

2.2 I contratti collettivi nazionali possono integrare le procedure e i criteri generali per l'attuazione di quanto previsto dai commi 1 e 2. Sono nulli gli accordi, gli atti o le clausole dei contratti collettivi in contrasto con le disposizioni di cui ai commi 1 e 2.

2.3 Al fine di favorire i processi di cui ai commi 1 e 2, è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un fondo destinato al miglioramento dell'allocazione del personale presso le pubbliche amministrazioni, con una dotazione di 15 milioni di euro per l'anno 2014 e di 30 milioni di euro a decorrere dall'anno 2015, da attribuire alle amministrazioni destinatarie dei predetti processi. Al fondo confluiscono, altresì, le risorse corrispondenti al cinquanta per cento del trattamento economico spettante al personale trasferito mediante versamento all'entrata dello Stato da parte dell'amministrazione cedente e corrispondente riassegnazione al fondo ovvero mediante contestuale riduzione dei trasferimenti statali all'amministrazione cedente. I criteri di utilizzo e le modalità di gestione delle risorse del fondo sono stabiliti con decreto del Presidente del Consiglio dei Ministri, di concerto con il Ministro dell'economia e delle finanze. In sede di prima applicazione, nell'assegnazione delle risorse vengono prioritariamente valutate le richieste finalizzate all'ottimale funzionamento degli uffici giudiziari che presentino rilevanti carenze di personale e conseguentemente alla piena applicazione della riforma delle province di cui alla legge 7 aprile 2014, n. 56. Le risorse sono assegnate alle amministrazioni di destinazione sino al momento di effettiva permanenza in servizio del personale oggetto delle procedure di cui ai commi 1 e 2.

2.4 Agli oneri derivanti dall'attuazione del comma 2.3, pari a 15 milioni di euro per l'anno 2014 e a 30 milioni di euro a decorrere dall'anno 2015, si provvede, quanto a 6 milioni di euro per l'anno 2014 e a 9 milioni di euro a decorrere dal 2015 mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 3, comma 97, della legge 24 dicembre 2007, n. 244, quanto a 9 milioni di euro a decorrere dal 2014 mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 14, del decreto-legge del 3 ottobre 2006, n. 262 convertito con modificazioni, dalla legge 24 novembre 2006, n. 286 e quanto a 12 milioni di euro a decorrere dal 2015 mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 527, della legge 27 dicembre 2006, n. 296. A decorrere dall'anno 2015, il fondo di cui al comma 2.3 può essere rideterminato

ai sensi dell'articolo 11, comma 3, lettera *d)*, della legge 31 dicembre 2009, n. 196. Il Ministro dell'economia e delle finanze è autorizzato ad apportare con propri decreti le occorrenti variazioni di bilancio per l'attuazione del presente articolo.

2-*bis*. Le amministrazioni, prima di procedere all'espletamento di procedure concorsuali, finalizzate alla copertura di posti vacanti in organico, devono attivare le procedure di mobilità di cui al comma 1, provvedendo, in via prioritaria, all'immissione in ruolo dei dipendenti, provenienti da altre amministrazioni, in posizione di comando o di fuori ruolo, appartenenti alla stessa area funzionale, che facciano domanda di trasferimento nei ruoli delle amministrazioni in cui prestano servizio. Il trasferimento è disposto, nei limiti dei posti vacanti, con inquadramento nell'area funzionale e posizione economica corrispondente a quella posseduta presso le amministrazioni di provenienza; il trasferimento può essere disposto anche se la vacanza sia presente in area diversa da quella di inquadramento assicurando la necessaria neutralità finanziaria.

2-*ter*. L'immissione in ruolo di cui al comma 2-*bis*, limitatamente alla Presidenza del Consiglio dei ministri e al Ministero degli affari esteri, in ragione della specifica professionalità richiesta ai propri dipendenti, avviene previa valutazione comparativa dei titoli di servizio e di studio, posseduti dai dipendenti comandati o fuori ruolo al momento della presentazione della domanda di trasferimento, nei limiti dei posti effettivamente disponibili.

2-*quater*. La Presidenza del Consiglio dei ministri, per fronteggiare le situazioni di emergenza in atto, in ragione della specifica professionalità richiesta ai propri dipendenti può procedere alla riserva di posti da destinare al personale assunto con ordinanza per le esigenze della Protezione civile e del servizio civile, nell'ambito delle procedure concorsuali di cui all'articolo 3, comma 59, della legge 24 dicembre 2003, n. 350, e all'articolo 1, comma 95, della legge 30 dicembre 2004, n. 311".

2-*quinquies*. Salvo diversa previsione, a seguito dell'iscrizione nel ruolo dell'amministrazione di destinazione, al dipendente trasferito per mobilità si applica esclusivamente il trattamento giuridico ed economico, compreso quello accessorio, previsto nei contratti collettivi vigenti nel comparto della stessa amministrazione.

2-*sexies*. Le pubbliche amministrazioni, per motivate esigenze organizzative, risultanti dai documenti di programmazione previsti all'articolo 6, possono utilizzare in assegnazione temporanea, con le modalità previste dai rispettivi ordinamenti, personale di altre amministrazioni per un periodo non superiore a tre anni, fermo restando quanto già previsto da norme speciali sulla materia, nonché il regime di spesa eventualmente previsto da tali norme e dal presente decreto.».

— Si riporta il testo dell'articolo 17, comma 14, della legge 15 maggio 1997, n. 127 (Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo):

«Art. 17 *(Ulteriori disposizioni in materia di semplificazione dell'attività amministrativa e di snellimento dei procedimenti di decisione e di controllo)*. — *Omissis*.14. Nel caso in cui disposizioni di legge o regolamentari dispongano l'utilizzazione presso le amministrazioni pubbliche di un contingente di personale in posizione di fuori ruolo o di comando, le amministrazioni di appartenenza sono tenute ad adottare il provvedimento di fuori ruolo o di comando entro quindici giorni dalla richiesta.*Omissis*.»

Note all'art. 13:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse

— Per i riferimenti del citato decreto-legge 14 giugno 2021, n. 82 si veda nelle note all'art. 1.

Note all'art. 14:

— Si riporta il testo dell'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144 (Misure urgenti per il contrasto del terrorismo internazionale) pubblicato nella *Gazzetta ufficiale* del 27 luglio 2005, n. 173, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, pubblicato nella *Gazzetta ufficiale* del 1° agosto 2005, n. 177.

«Art. 7-*bis (Sicurezza telematica)*. — 1. Ferme restando le competenze dei Servizi informativi e di sicurezza, di cui agli articoli 4 e 6 della legge 24 ottobre 1977, n. 801, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione assicura i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale individuate con decreto del Ministro dell'interno, operando mediante collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate.

2. Per le finalità di cui al comma 1 e per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, gli ufficiali di polizia giudiziaria appartenenti all'organo di cui al comma 1 possono svolgere le attività di cui all'articolo 4, commi 1 e 2, del decreto-legge 18 ottobre 2001, n. 374, convertito, con modificazioni, dalla legge 15 dicembre 2001, n. 438, e quelle di cui all'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, anche a richiesta o in collaborazione con gli organi di polizia giudiziaria ivi indicati.».

— Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) è pubblicato nella GUUE del 4 maggio 2016, n. 119, serie L.

— Il regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008 che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 è pubblicato nella GUUE del 9 aprile 2008, n. 97, serie L.

— Il regolamento (UE) 2018/1139, del Parlamento europeo e del Consiglio, del 4 luglio 2018 recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio è pubblicato nella GUUE del 22 agosto 2018 n. 212 serie L.

— Il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE è pubblicato nella GUUE del 28 agosto 2014, n. 257, serie L.

— Per la direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche (rifusione) si veda nelle note alle premesse.

— Per i riferimenti all'art. 7, comma 5, del citato decreto-legge 14 giugno 2021, n. 82 si veda nelle note all'art. 9.

— Per il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 si veda nelle note alle premesse.

— Per la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio si veda nelle note alle premesse.

Note all'art. 15:

— Per i riferimenti all'art. 7, comma 1, lettera *s)*, del decreto-legge 14 giugno 2021, n. 82, si veda nelle note all'art. 9.

Note all'art. 16:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 17:

— Si riporta il testo degli articoli 4, 6 e 7 della legge n. 124 del 2007 (Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto), pubblicata nella *Gazzetta ufficiale* del 13 agosto 2007, n. 187:

«Art. 4 *(Dipartimento delle informazioni per la sicurezza)*. — 1. Per lo svolgimento dei compiti di cui al comma 3 è istituito, presso la Presidenza del Consiglio dei ministri, il Dipartimento delle informazioni per la sicurezza (DIS).

2. Il Presidente del Consiglio dei ministri e l'Autorità delegata, ove istituita, si avvalgono del DIS per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza, nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza.

3. Il DIS svolge i seguenti compiti:

a) coordina l'intera attività di informazione per la sicurezza, verificando altresì i risultati delle attività svolte dall'AISE e dall'AISI, ferma restando la competenza dei predetti servizi relativamente alle attività di ricerca informativa e di collaborazione con i servizi di sicurezza degli Stati esteri;

b) è costantemente informato delle operazioni di competenza dei servizi di informazione per la sicurezza e trasmette al Presidente del Consiglio dei ministri le informative e le analisi prodotte dal Sistema di informazione per la sicurezza;

c) raccoglie le informazioni, le analisi e i rapporti provenienti dai servizi di informazione per la sicurezza, dalle Forze armate e di polizia, dalle amministrazioni dello Stato e da enti di ricerca anche privati; ferma l'esclusiva competenza dell'AISE e dell'AISI per l'elaborazione dei rispettivi piani di ricerca operativa, elabora analisi strategiche o relative a particolari situazioni; formula valutazioni e previsioni, sulla scorta dei contributi analitici settoriali dell'AISE e dell'AISI;

d) elabora, anche sulla base delle informazioni e dei rapporti di cui alla lettera *c)*, analisi globali da sottoporre al CISR, nonché progetti di ricerca informativa, sui quali decide il Presidente del Consiglio dei ministri, dopo avere acquisito il parere del CISR;

d-*bis*) sulla base delle direttive di cui all'articolo 1, comma 3-*bis*, nonché delle informazioni e dei rapporti di cui alla lettera *c)* del presente comma, coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

e) promuove e garantisce, anche attraverso riunioni periodiche, lo scambio informativo tra l'AISE, l'AISI e le Forze di polizia; comunica al Presidente del Consiglio dei ministri le acquisizioni provenienti dallo scambio informativo e i risultati delle riunioni periodiche;

f) trasmette, su disposizione del Presidente del Consiglio dei ministri, sentito il CISR, informazioni e analisi ad amministrazioni pubbliche o enti, anche ad ordinamento autonomo, interessati all'acquisizione di informazioni per la sicurezza;

g) elabora, d'intesa con l'AISE e l'AISI, il piano di acquisizione delle risorse umane e materiali e di ogni altra risorsa comunque strumentale all'attività dei servizi di informazione per la sicurezza, da sottoporre all'approvazione del Presidente del Consiglio dei ministri;

h) sentite l'AISE e l'AISI, elabora e sottopone all'approvazione del Presidente del Consiglio dei ministri lo schema del regolamento di cui all'articolo 21, comma 1;

i) esercita il controllo sull'AISE e sull'AISI, verificando la conformità delle attività di informazione per la sicurezza alle leggi e ai regolamenti, nonché alle direttive e alle disposizioni del Presidente del Consiglio dei ministri. Per tale finalità, presso il DIS è istituito un ufficio ispettivo le cui modalità di organizzazione e di funzionamento sono definite con il regolamento di cui al comma 7. Con le modalità previste da tale regolamento è approvato annualmente, previo parere del Comitato parlamentare di cui all'articolo 30, il piano annuale delle attività dell'ufficio ispettivo. L'ufficio ispettivo, nell'ambito delle competenze definite con il predetto regolamento, può svolgere, anche a richiesta del direttore generale del DIS, autorizzato dal Presidente del Consiglio dei ministri, inchieste interne su specifici episodi e comportamenti verificatisi nell'ambito dei servizi di informazione per la sicurezza;

l) assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei Ministri con apposito regolamento adottato ai sensi dell'articolo 1, comma 2, ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione;

m) cura le attività di promozione e diffusione della cultura della sicurezza e la comunicazione istituzionale;

n) impartisce gli indirizzi per la gestione unitaria del personale di cui all'articolo 21, secondo le modalità definite dal regolamento di cui al comma 1 del medesimo articolo;

n-*bis*) gestisce unitariamente, ferme restando le competenze operative dell'AISE e dell'AISI, gli approvvigionamenti e i servizi logistici comuni.

4. Fermo restando quanto previsto dall'articolo 118-*bis* del codice di procedura penale, introdotto dall'articolo 14 della presente legge, qualora le informazioni richieste alle Forze di polizia, ai sensi delle lettere *c)* ed *e)* del comma 3 del presente articolo, siano relative a indagini di polizia giudiziaria, le stesse, se coperte dal segreto di cui all'articolo 329 del codice di procedura penale, possono essere acquisite solo previo nulla osta della autorità giudiziaria competente. L'autorità giudiziaria può trasmettere gli atti e le informazioni anche di propria iniziativa.

5. La direzione generale del DIS è affidata ad un dirigente di prima fascia o equiparato dell'amministrazione dello Stato, la cui nomina e revoca spettano in via esclusiva al Presidente del Consiglio dei ministri, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio. Per quanto previsto dalla presente legge, il direttore del DIS è il diretto referente del Presidente del Consiglio dei ministri e dell'Autorità delegata, ove istituita, salvo quanto previsto dall'articolo 6, comma 5, e dall'articolo 7, comma 5, ed è gerarchicamente e funzionalmente sovraordinato al personale del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento.

6. Il Presidente del Consiglio dei ministri, sentito il direttore generale del DIS, nomina uno o più vice direttori generali; il direttore generale affida gli altri incarichi nell'ambito del Dipartimento, ad eccezione degli incarichi il cui conferimento spetta al Presidente del Consiglio dei ministri.

7. L'ordinamento e l'organizzazione del DIS e degli uffici istituiti nell'ambito del medesimo Dipartimento sono disciplinati con apposito regolamento.

8. Il regolamento previsto dal comma 7 definisce le modalità di organizzazione e di funzionamento dell'ufficio ispettivo di cui al comma 3, lettera *i)*, secondo i seguenti criteri:

a) agli ispettori è garantita piena autonomia e indipendenza di giudizio nell'esercizio delle funzioni di controllo;

b) salva specifica autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, i controlli non devono interferire con le operazioni in corso;

c) sono previste per gli ispettori specifiche prove selettive e un'adeguata formazione;

d) non è consentito il passaggio di personale dall'ufficio ispettivo ai servizi di informazione per la sicurezza;

e) gli ispettori, previa autorizzazione del Presidente del Consiglio dei ministri o dell'Autorità delegata, ove istituita, possono accedere a tutti gli atti conservati presso i servizi di informazione per la sicurezza e presso il DIS; possono altresì acquisire, tramite il direttore generale del DIS, altre informazioni da enti pubblici e privati.».

«Articolo 6 *(Agenzia informazioni e sicurezza esterna)*. — 1. È istituita l'Agenzia informazioni e sicurezza esterna (AISE), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica, anche in attuazione di accordi internazionali, dalle minacce provenienti dall'estero.

2. Spettano all'AISE, inoltre, le attività in materia di controproliferazione concernenti i materiali strategici, nonché le attività di informazione per la sicurezza, che si svolgono al di fuori del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISE individuare e contrastare al di fuori del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISE può svolgere operazioni sul territorio nazionale soltanto in collaborazione con l'AISI, quando tali operazioni siano strettamente connesse ad attività che la stessa AISE svolge all'estero. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISE risponde al Presidente del Consiglio dei ministri.

6. L'AISE informa tempestivamente e con continuità il Ministro della difesa, il Ministro degli affari esteri e il Ministro dell'interno per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri, con proprio decreto, nomina e revoca il direttore dell'AISE, scelto tra dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

8. Il direttore dell'AISE riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISE, uno o più vice direttori. Il direttore dell'AISE affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISE sono disciplinati con apposito regolamento.».

«Articolo 7 (Agenzia informazioni e sicurezza interna). — 1. È istituita l'Agenzia informazioni e sicurezza interna (AISI), alla quale è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili a difendere, anche in attuazione di accordi internazionali, la sicurezza interna della Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica.

2. Spettano all'AISI le attività di informazione per la sicurezza, che si svolgono all'interno del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia.

3. È, altresì, compito dell'AISI individuare e contrastare all'interno del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

4. L'AISI può svolgere operazioni all'estero soltanto in collaborazione con l'AISE, quando tali operazioni siano strettamente connesse ad attività che la stessa AISI svolge all'interno del territorio nazionale. A tal fine il direttore generale del DIS provvede ad assicurare le necessarie forme di coordinamento e di raccordo informativo, anche al fine di evitare sovrapposizioni funzionali o territoriali.

5. L'AISI risponde al Presidente del Consiglio dei ministri.

6. L'AISI informa tempestivamente e con continuità il Ministro dell'interno, il Ministro degli affari esteri e il Ministro della difesa per i profili di rispettiva competenza.

7. Il Presidente del Consiglio dei ministri nomina e revoca, con proprio decreto, il direttore dell'AISI, scelto tra i dirigenti di prima fascia o equiparati dell'amministrazione dello Stato, sentito il CISR. L'incarico ha la durata massima di otto anni ed è conferibile, senza soluzione di continuità, anche con provvedimenti successivi, ciascuno dei quali di durata non superiore al quadriennio.

8. Il direttore dell'AISI riferisce costantemente sull'attività svolta al Presidente del Consiglio dei ministri o all'Autorità delegata, ove istituita, per il tramite del direttore generale del DIS. Riferisce direttamente al Presidente del Consiglio dei ministri in caso di urgenza o quando altre particolari circostanze lo richiedano, informandone senza ritardo il direttore generale del DIS; presenta al CISR, per il tramite del direttore generale del DIS, un rapporto annuale sul funzionamento e sull'organizzazione dell'Agenzia.

9. Il Presidente del Consiglio dei ministri nomina e revoca, sentito il direttore dell'AISI, uno o più vice direttori. Il direttore dell'AISI affida gli altri incarichi nell'ambito dell'Agenzia.

10. L'organizzazione e il funzionamento dell'AISI sono disciplinati con apposito regolamento.».

Note all'art. 18:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse

— Per il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio si vede nelle note all'art. 2.

Note all'art. 19:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 20:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 21:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 22:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 25:

— Per i riferimenti all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144 (Misure urgenti per il contrasto del terrorismo internazionale) pubblicato nella *Gazzetta ufficiale* del 27 luglio 2005, n. 173, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, si veda nelle note all'art. 14.

Note all'art. 27:

— Per il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») si veda nelle note alle premesse.

Note all'art. 28:

— Per il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio si veda nelle note all'art. 2.

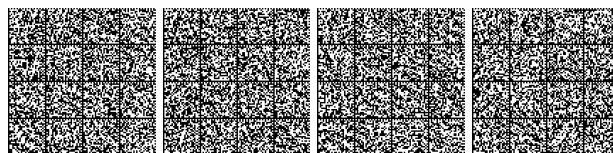
— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 33:

— Si riporta il testo dell'art. 1, commi 2 e 2-*bis*, del citato decreto-legge n. 105/2019, convertito con modificazioni dalla legge 18 novembre 2019, n. 133:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1. (*Omissis*).

2. Entro quattro mesi dalla data di entrata in vigore della legge di conversione del presente decreto, con decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la cybersicurezza (CIC):

a) sono definiti modalità e criteri procedurali di individuazione di amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e

degli obblighi previsti dal presente articolo; ai fini dell'individuazione, fermo restando che per gli Organismi di informazione per la sicurezza si applicano le norme previste dalla legge 3 agosto 2007, n. 124, si procede sulla base dei seguenti criteri:

1) il soggetto esercita una funzione essenziale dello Stato, ovvero assicura un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;

2) l'esercizio di tale funzione o la prestazione di tale servizio dipende da reti, sistemi informativi e servizi informatici;

2-*bis*) l'individuazione avviene sulla base di un criterio di gradualità, tenendo conto dell'entità del pregiudizio per la sicurezza nazionale che, in relazione alle specificità dei diversi settori di attività, può derivare dal malfunzionamento, dall'interruzione, anche parziali, ovvero dall'utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici predetti;

b) sono definiti, sulla base di un'analisi del rischio e di un criterio di gradualità che tenga conto delle specificità dei diversi settori di attività, i criteri con i quali i soggetti di cui al comma 2-*bis* predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 1, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica, fermo restando che, per le reti, i sistemi informativi e i servizi informatici attinenti alla gestione delle informazioni classificate, si applica quanto previsto dal regolamento adottato ai sensi dell'articolo 4, comma 3, lettera *l)*, della legge 3 agosto 2007, n. 124; all'elaborazione di tali criteri provvede, adottando opportuni moduli organizzativi, il Tavolo interministeriale di cui all'articolo 6 del regolamento di cui al decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131; entro sei mesi dalla data della comunicazione, prevista dal comma 2-*bis*, a ciascuno dei soggetti iscritti nell'elenco di cui al medesimo comma, i soggetti pubblici e quelli di cui all'articolo 29 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, nonché quelli privati, di cui al citato comma 2-*bis*, trasmettono tali elenchi all'Agenzia per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI) ai fini dell'esercizio delle funzioni istituzionali previste dagli articoli 1, comma 3-*bis*, 4, 6 e 7 della legge n. 124 del 2007, nonché l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, accedono a tali elenchi per il tramite della piattaforma digitale di cui all'articolo 9, comma 1, del regolamento di cui al decreto del Presidente del Consiglio dei ministri n. 131 del 2020, costituita presso l'Agenzia per la cybersicurezza nazionale.

2-*bis*. L'elencazione dei soggetti individuati ai sensi del comma 2, lettera *a)*, è contenuta in un atto amministrativo, adottato dal Presidente del Consiglio dei ministri, su proposta del CIC, entro trenta giorni dalla data di entrata in vigore del decreto del Presidente del Consiglio dei ministri di cui al comma 2. Il predetto atto amministrativo, per il quale è escluso il diritto di accesso, non è soggetto a pubblicazione, fermo restando che a ciascun soggetto è data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco. L'aggiornamento del predetto atto amministrativo è effettuato con le medesime modalità di cui al presente comma.

2-*ter* - 19-*ter*. (*Omissis*).»

Note all'art. 38:

— Per la raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese si veda nelle note alle premesse.

— Si riporta il testo dell'articolo 8-*bis* della legge 24 novembre del 1981, n. 689 (Modifiche al sistema penale), pubblicata nella *Gazzetta Ufficiale* del 30 novembre 1981, n. 329:

«Art. 8-*bis (Reiterazioni delle violazioni)*. — Salvo quanto previsto da speciali disposizioni di legge, si ha reiterazione quando, nei cinque anni successivi alla commissione di una violazione amministrativa, accertata con provvedimento esecutivo, lo stesso soggetto commette un'altra violazione della stessa indole. Si ha reiterazione anche quando più violazioni della stessa indole commesse nel quinquennio sono accertate con unico provvedimento esecutivo.

Si considerano della stessa indole le violazioni della medesima disposizione e quelle di disposizioni diverse che, per la natura dei fatti che le costituiscono o per le modalità della condotta, presentano una sostanziale omogeneità o caratteri fondamentali comuni.

La reiterazione è specifica se è violata la medesima disposizione.

Le violazioni amministrative successive alla prima non sono valutate, ai fini della reiterazione, quando sono commesse in tempi ravvicinati e riconducibili ad una programmazione unitaria.

La reiterazione determina gli effetti che la legge espressamente stabilisce. Essa non opera nel caso di pagamento in misura ridotta.

Gli effetti conseguenti alla reiterazione possono essere sospesi fino a quando il provvedimento che accerta la violazione precedentemente commessa sia divenuto definitivo. La sospensione è disposta dall'autorità amministrativa competente, o in caso di opposizione dal giudice, quando possa derivare grave danno.

Gli effetti della reiterazione cessano di diritto, in ogni caso, se il provvedimento che accerta la precedente violazione è annullato.».

— Si riporta il testo dell'articolo 18 del citato decreto-legge 14 giugno 2021, n. 82:

«Art. 18 *(Disposizioni finanziarie)*. — 1. Per l'attuazione degli articoli da 5 a 7 è istituito, nello stato di previsione del Ministero dell'economia e delle finanze, un apposito capitolo con una dotazione di 2.000.000 di euro per l'anno 2021, 41.000.000 di euro per l'anno 2022, 70.000.000 di euro per l'anno 2023, 84.000.000 di euro per l'anno 2024, 100.000.000 di euro per l'anno 2025, 110.000.000 di euro per l'anno 2026 e 122.000.000 di euro annui a decorrere dall'anno 2027.

2. Agli oneri di cui al comma 1, si provvede mediante corrispondente riduzione del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190.

3. Le risorse iscritte sui bilanci delle amministrazioni interessate, correlate alle funzioni ridefinite ai sensi del presente decreto a decorrere dall'inizio del funzionamento dell'Agenzia di cui all'articolo 5, sono accertate, anche in conto residui, con decreto del Ministro dell'economia e delle finanze, di concerto con i Ministri responsabili, e portate ad incremento del Fondo di cui all'articolo 1, comma 200, della legge 23 dicembre 2014, n. 190, anche mediante versamento all'entrata del bilancio dello Stato e successiva riassegnazione alla spesa.

4. I proventi di cui all'articolo 11, comma 2, sono versati all'entrata del bilancio dello Stato, per essere riassegnati al capitolo di cui al comma 1 del presente articolo.

5. Ai fini dell'immediata attuazione delle disposizioni del presente decreto il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, anche in conto residui, le occorrenti variazioni di bilancio.».

Note all'art. 39:

— Per i riferimenti alla direttiva (UE) 2022/2555 misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) si veda nelle note alle premesse.

Note all'art. 40:

— Si riporta il testo dell'art. 17 della citata legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri):

«Art. 17 *(Regolamenti)*. — 1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il parere del Consiglio di Stato che deve pronunziarsi entro novanta giorni dalla richiesta, possono essere emanati regolamenti per disciplinare:

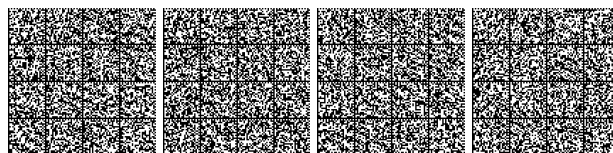
a) l'esecuzione delle leggi e dei decreti legislativi nonché dei regolamenti comunitari;

b) l'attuazione e l'integrazione delle leggi e dei decreti legislativi recanti norme di principio, esclusi quelli relativi a materie riservate alla competenza regionale;

c) le materie in cui manchi la disciplina da parte di leggi o di atti aventi forza di legge, sempre che non si tratti di materie comunque riservate alla legge;

d) l'organizzazione ed il funzionamento delle amministrazioni pubbliche secondo le disposizioni dettate dalla legge;

e).

2. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, sentito il Consiglio di Stato e previo parere delle Commissioni parlamentari competenti in materia, che si

pronunciano entro trenta giorni dalla richiesta, sono emanati i regolamenti per la disciplina delle materie, non coperte da riserva assoluta di legge prevista dalla Costituzione, per le quali le leggi della Repubblica, autorizzando l'esercizio della potestà regolamentare del Governo, determinano le norme generali regolatrici della materia e dispongono l'abrogazione delle norme vigenti, con effetto dall'entrata in vigore delle norme regolamentari.

3. Con decreto ministeriale possono essere adottati regolamenti nelle materie di competenza del Ministro o di autorità sottordinate al Ministro, quando la legge espressamente conferisca tale potere. Tali regolamenti, per materie di competenza di più ministri, possono essere adottati con decreti interministeriali, ferma restando la necessità di apposita autorizzazione da parte della legge. I regolamenti ministeriali ed interministeriali non possono dettare norme contrarie a quelle dei regolamenti emanati dal Governo. Essi debbono essere comunicati al Presidente del Consiglio dei ministri prima della loro emanazione.

4. I regolamenti di cui al comma 1 ed i regolamenti ministeriali ed interministeriali, che devono recare la denominazione di "regolamento", sono adottati previo parere del Consiglio di Stato, sottoposti al visto ed alla registrazione della Corte dei conti e pubblicati nella *Gazzetta Ufficiale*.

4-*bis*. L'organizzazione e la disciplina degli uffici dei Ministeri sono determinate, con regolamenti emanati ai sensi del comma 2, su proposta del Ministro competente d'intesa con il Presidente del Consiglio dei ministri e con il Ministro del tesoro, nel rispetto dei principi posti dal decreto legislativo 3 febbraio 1993, n. 29, e successive modificazioni, con i contenuti e con l'osservanza dei criteri che seguono:

a) riordino degli uffici di diretta collaborazione con i ministri ed i Sottosegretari di Stato, stabilendo che tali uffici hanno esclusive competenze di supporto dell'organo di direzione politica e di raccordo tra questo e l'amministrazione;

b) individuazione degli uffici di livello dirigenziale generale, centrali e periferici, mediante diversificazione tra strutture con funzioni finali e con funzioni strumentali e loro organizzazione per funzioni omogenee e secondo criteri di flessibilità eliminando le duplicazioni funzionali;

c) previsione di strumenti di verifica periodica dell'organizzazione e dei risultati;

d) indicazione e revisione periodica della consistenza elle piante organiche;

e) previsione di decreti ministeriali di natura non regolamentare per la definizione dei compiti delle unità dirigenziali nell'ambito degli uffici dirigenziali generali.

4-*ter*. Con regolamenti da emanare ai sensi del comma 1 del presente articolo, si provvede al periodico riordino delle disposizioni regolamentari vigenti, alla ricognizione di quelle che sono state oggetto di abrogazione implicita e all'espressa abrogazione di quelle che hanno esaurito la loro funzione o sono prive di effettivo contenuto normativo o sono comunque obsolete.».

— Si riporta il testo dell'articolo 4 del citato decreto-legge 14 giugno 2021, n. 82:

«Art. 4 *(Comitato interministeriale per la cybersicurezza)*. — 1. Presso la Presidenza del Consiglio dei ministri è istituito il Comitato interministeriale per la cybersicurezza (CIC), con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza.

2. Il Comitato:

a) propone al Presidente del Consiglio dei ministri gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza nazionale;

b) esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza;

c) promuove l'adozione delle iniziative necessarie per favorire l'efficace collaborazione, a livello nazionale e internazionale, tra i soggetti istituzionali e gli operatori privati interessati alla cybersicurezza, nonché per la condivisione delle informazioni e per l'adozione di migliori pratiche e di misure rivolte all'obiettivo della cybersicurezza e allo sviluppo industriale, tecnologico e scientifico in materia di cybersicurezza;

d) esprime il parere sul bilancio preventivo e sul bilancio consuntivo dell'Agenzia per la cybersicurezza nazionale.

3. Il Comitato è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri e della cooperazione internazionale, dal Ministro dell'interno, dal Ministro della giustizia, dal Ministro della difesa, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico, dal Ministro della transizione ecologica, dal Ministro dell'università e della ricerca, dal Ministro delegato per l'innovazione tecnologica e la transizione digitale e dal Ministro delle infrastrutture e della mobilità sostenibili.

4. Il direttore generale dell'Agenzia per la cybersicurezza nazionale svolge le funzioni di segretario del Comitato.

5. Il Presidente del Consiglio dei ministri può chiamare a partecipare alle sedute del Comitato, anche a seguito di loro richiesta, senza diritto di voto, altri componenti del Consiglio dei ministri, nonché altre autorità civili e militari di cui, di volta in volta, ritenga necessaria la presenza in relazione alle questioni da trattare.

6. Il Comitato svolge altresì le funzioni già attribuite al Comitato interministeriale per la sicurezza della Repubblica (CISR), di cui all'articolo 5 della legge 3 agosto 2007, n. 124, dal decreto-legge perimetro e dai relativi provvedimenti attuativi, fatta eccezione per quelle previste dall'articolo 5 del medesimo decreto-legge perimetro.».

Note all'art. 41:

— Il decreto legislativo 18 maggio 2018, n. 65, abrogato, a decorrere dal 18 ottobre 2024 dal presente decreto, reca: «Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione», ed è pubblicato nella *Gazzetta Ufficiale* 9 giugno 2018, n. 132.

— Si riporta il testo degli articoli 7, comma 8, e 8, comma 10, del citato decreto legislativo 18 maggio 2018, n. 65, abrogati, a decorrere dal 1° gennaio 2025 dal presente decreto:

«Art. 7 *(Autorità nazionale competente e punto di contatto unico)*. — 1. – 7. *Omissis*.

8. Agli oneri derivanti dal presente articolo, pari a 1.300.000 euro annui a decorrere dall'anno 2018, si provvede ai sensi dell'articolo 22.»

«Art. 8 *(Gruppi di intervento per la sicurezza informatica in caso di incidente – CSIRT)*. — 1. – 9. *Omissis*.

10. Per le spese relative al funzionamento del CSIRT Italia è autorizzata la spesa di 2.000.000 di euro annui a decorrere dall'anno 2020. A tali oneri si provvede ai sensi dell'articolo 22.».

— I capi IV e V del citato decreto legislativo 18 maggio 2018, n. 65 recano, rispettivamente, «Sicurezza della rete e dei sistemi informativi degli operatori di servizi essenziali» e «Sicurezza della rete e dei sistemi informativi dei fornitori di servizi digitali».

— Si riporta il testo dell'articolo, 2, comma 1, lettera *h)*, dell'articolo 30, comma 26, e degli articoli 40 e 41 del decreto legislativo 1° agosto 2003, n. 259, (Codice delle comunicazioni elettroniche), pubblicato in *Gazzetta Ufficiale* il 15 settembre 2003, abrogati dal presente provvedimento:

«Art. 2 *(Definizioni)*. — 1. Ai fini del presente decreto si intende per:

a) - g). *Omissis*.

h) apparecchiature terminali: apparecchiature terminali quali definite all'articolo 1, comma 1), del decreto legislativo 26 ottobre 2010 n. 198;

i) – dddd). *Omissis*.».

«Articolo 30 *(Sanzioni)*. — 1.- 25. *Omissis*.

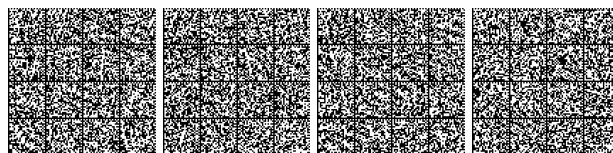
26. Salvo che il fatto non costituisca reato, l'inosservanza delle disposizioni in materia di sicurezza informatica è punita, con una sanzione amministrativa pecuniaria:

a) da euro 250.000 a euro 1.500.000 per l'inosservanza delle misure di sicurezza di cui all'articolo 40, comma 3, lettera *a)*;

b) da euro 300.000 ad euro 1.800.000 per la mancata comunicazione di ogni incidente significativo di cui all'articolo 40, comma 3, lettera *b)*;

c) da euro 200.000 a euro 1.000.000 per la mancata fornitura delle informazioni necessarie per valutare la sicurezza di cui all'articolo 40, comma 3, lettera *a)*.

27. – 27-*quinquies*. *Omissis*.».

«Art. 40 (Sicurezza delle reti e dei servizi). — 1. L'Agenzia, sentito il Ministero, per quanto di rispettiva competenza e tenuto conto delle misure tecniche e organizzative che possono essere adottate dalla

Commissione europea, ai sensi dell'articolo 40, paragrafo 5, della direttiva (UE) 2018/1972, individua:

a) adeguate e proporzionate misure di natura tecnica e organizzativa per gestire i rischi per la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, assicurando un livello di sicurezza adeguato al rischio esistente, tenuto conto delle attuali conoscenze in materia. Tali misure, che possono comprendere, se del caso, il ricorso a tecniche di crittografia, sono anche finalizzate a prevenire e limitare le conseguenze per gli utenti, le reti interconnesse e gli altri servizi, degli incidenti che pregiudicano la sicurezza;

b) i casi in cui gli incidenti di sicurezza siano da considerarsi significativi ai fini del corretto funzionamento delle reti o dei servizi.

2. Nella determinazione dei casi di cui al comma 1, lettera *b)*, l'Agenzia considera i seguenti parametri, se disponibili:

a) il numero di utenti interessati dall'incidente di sicurezza;

b) la durata dell'incidente di sicurezza;

c) la diffusione geografica della zona interessata dall'incidente di sicurezza;

d) la misura in cui è colpito il funzionamento della rete o del servizio;

e) la portata dell'incidenza sulle attività economiche e sociali.

3. Le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico:

a) adottano le misure individuate dall'Agenzia di cui al comma 1, lettera *a)*;

b) comunicano all'Agenzia e al Computer Security Incident Response Team (CSIRT), istituito ai sensi dell'articolo 8 del decreto legislativo 18 maggio 2018, n. 65, ogni significativo incidente di sicurezza secondo quanto previsto dal comma 1, lettera *b)*.

4. L'Agenzia può informare il pubblico o imporre all'impresa di farlo, ove accerti che la divulgazione della notizia dell'incidente di sicurezza di cui al comma 1, lettera *b)*, sia nell'interesse pubblico. Se del caso, l'Agenzia informa le Autorità competenti degli altri Stati membri e l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA).

5. L'Agenzia, anche avvalendosi del CSIRT, provvede direttamente o per il tramite dei fornitori di reti e servizi di comunicazione elettronica ad informare gli utenti potenzialmente interessati da minaccia particolare e significativa di incidenti di sicurezza, riguardo a eventuali misure di protezione o rimedi cui possono ricorrere.

6. L'Agenzia trasmette ogni anno alla Commissione europea e all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione una relazione sintetica delle notifiche ricevute e delle azioni adottate conformemente al presente articolo.

7. L'Agenzia, nelle tematiche di cybersicurezza, fatta eccezione per gli ambiti in cui la legge attribuisce specifiche competenze ad altre amministrazioni, collabora con le autorità competenti degli altri Stati membri e con i competenti organismi internazionali e dell'Unione europea al fine di definire procedure e norme che garantiscano la sicurezza dei servizi.

8. In caso di notifica di incidente di sicurezza che determini anche una violazione di dati personali, l'Agenzia fornisce, senza ritardo, al Garante per la protezione dei dati personali le informazioni utili ai fini di cui all'articolo 33 del Regolamento UE 2016/679.».

«Art. 41 *(Attuazione e controllo)*. — 1. Le misure adottate ai fini dell'attuazione del presente articolo e dell'articolo 40 sono approvate con provvedimento dell'Agenzia.

2. I fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazioni elettroniche accessibili al pubblico adottano le istruzioni vincolanti eventualmente impartite dall'Agenzia, anche con riferimento alle misure necessarie per porre rimedio a un incidente di sicurezza o per evitare che si verifichi nel caso in cui sia stata individuata una minaccia significativa.

3. Ai fini del controllo del rispetto dell'articolo 40 le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico sono tenute a:

a) fornire all'Agenzia le informazioni necessarie per valutare la sicurezza delle loro reti e dei loro servizi, in particolare i documenti relativi alle politiche di sicurezza;

b) sottostare a verifiche di sicurezza effettuate dall'Agenzia o da un organismo qualificato indipendente designato dalla medesima Agenzia. L'impresa si assume l'onere finanziario della verifica.

4. L'Agenzia ha la facoltà di indagare i casi di mancata conformità nonché i loro effetti sulla sicurezza delle reti e dei servizi. I fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazioni elettroniche accessibili al pubblico che indirizzano o raccolgono traffico per servizi offerti sul territorio nazionale sono tenuti a fornire le informazioni e i dati necessari alle indagini.

5. L'Agenzia, se del caso, consulta l'Autorità, le Autorità di contrasto nazionali, il Garante per la protezione dei dati personali, e coopera con esse.

6. Nel caso in cui l'Agenzia riscontri il mancato rispetto del presente articolo e dell'articolo 40 ovvero delle disposizioni attuative previste dai commi 1 e 2 da parte delle imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, si applicano le sanzioni di cui all'articolo 30, commi da 2 a 21.».

Note all'art. 43:

— Per il testo dell'art. 1, del decreto legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, come modificato dal presente decreto, si veda nelle note all'art. 2.

- Si riporta il testo dell'art.7, del citato decreto-legge 14 giugno 2021, n. 82, come modificato dal presente decreto:

« Art. 7. Funzioni dell'Agenzia per la cybersicurezza nazionale

1. L'agenzia:

(*Omissis*).

d) è Autorità nazionale competente NIS e Punto di contatto unico NIS di cui all'articolo 2, comma 1, lettera d) *ed* e)*, del decreto legislativo NIS, a tutela dell'unità giuridica dell'ordinamento*;

d-bis*) è Autorità nazionale di gestione delle crisi informatiche di cui all'articolo 2, comma 1, lettera* g) *del decreto legislativo NIS*;

d-ter*) è CSIRT nazionale, denominato CSIRT Italia, di cui all'articolo 2, comma1, lettera* i)*, del decreto legislativo NIS»*;

(*Omissis*).

n) sviluppa capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici, anche attraverso il *CSIRT Italia, di cui all'articolo 2, comma1, lettera i)* del decreto legislativo NIS. A tale fine, promuove iniziative di partenariato pubblico-privato per rendere effettive tali capacità;

n-*bis*) nell'ambito delle funzioni di cui al primo periodo della lettera *n)*, svolge ogni attività diretta all'analisi e al supporto per il contenimento e il ripristino dell'operatività dei sistemi compromessi, con la collaborazione dei soggetti pubblici o privati che hanno subito incidenti di sicurezza informatica o attacchi informatici. La mancata collaborazione di cui al primo periodo è valutata ai fini dell'applicazione delle sanzioni previste dall'articolo 1, commi 10 e 14, del decreto-legge perimetro, per i soggetti di cui all'articolo 1, comma 2-*bis*, del medesimo decreto-legge perimetro, i soggetti essenziali e *i soggetti importanti di cui all'art. 6 del decreto legislativo NIS* e di cui all'articolo 40, comma 3, alinea, del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1° agosto 2003, n. 259; restano esclusi gli organi dello Stato preposti alla prevenzione, all'accertamento e alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, nonché gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124;

(*Omissis*).

1-*bis*. Anche ai fini dell'esercizio delle funzioni di cui al comma 1, lettere *r), s), t), u), v), z)* e *aa)*, presso l'Agenzia è istituito, con funzioni di consulenza e di proposta, un Comitato tecnico-scientifico, presieduto dal direttore generale della medesima Agenzia, o da un dirigente da lui delegato, e composto da personale della stessa Agenzia e da qualificati rappresentanti dell'industria, degli enti di ricerca, dell'accademia e delle associazioni del settore della sicurezza, designati con decreto del Presidente del Consiglio dei ministri. La composizione e l'organizzazione del Comitato tecnico-scientifico sono disciplinate secondo le modalità e i criteri definiti dal regolamento di cui all'articolo 6, comma 1.Per la partecipazione al Comitato tecnico-scientifico non sono previsti gettoni di presenza, compensi o rimborsi di spese.

2. Nell'ambito dell'Agenzia sono nominati, con decreto del Presidente del Consiglio dei ministri, il rappresentante nazionale, e il suo sostituto, nel Consiglio di direzione del Centro europeo di competenza per la cybersicurezza nell'ambito industriale, tecnologico e della ricerca, ai sensi dell'articolo 12 del regolamento (UE) 2021/887.

3. (*Abrogato*).

4. Il Centro di valutazione e certificazione nazionale, istituito presso il Ministero dello sviluppo economico, è trasferito presso l'Agenzia.

5. Nel rispetto delle competenze del Garante per la protezione dei dati personali, l'Agenzia, per le finalità di cui al presente decreto, consulta il Garante e collabora con esso, anche in relazione agli incidenti che comportano violazioni di dati personali. L'Agenzia e il Garante possono stipulare appositi protocolli d'intenti che definiscono altresì le modalità della loro collaborazione nell'ambito delle risorse disponibili a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica.»

— L'articolo 15, del citato decreto-legge 14 giugno 2021, n. 82, come abrogato dal presente decreto, recava: «Art. 15. *(Modificazioni al decreto legislativo NIS)*».

— Si riporta il testo dell'art. 1 del citato decreto-legge 21 settembre 2019, n. 105 convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, come modificato dal presente decreto:

«Art. 1 *(Perimetro di sicurezza nazionale cibernetica)*. — 1. – 3. (*Omissis*).

3-*bis*. (*abrogato*).

4. – 7. (*Omissis*).

8. La notifica d'incidente ai sensi del comma 3, lettera *a)*, effettuata dai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che rientrano nell'ambito di applicazione del decreto legislativo di recepimento della direttiva (UE) 2022/2555 assolve agli obblighi in materia di notifica di incidente di cui all'articolo 25 del decreto legislativo medesimo.;

*8-*bis. *Ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica che non sono individuati come soggetti essenziali o importanti ai sensi degli articoli 3 e 6 del decreto legislativo di recepimento della direttiva (UE) 2022/2555, si applicano gli obblighi di cui al capo IV e le attività ispettive e sanzionatorie di cui al capo V previste per i soggetti essenziali ai sensi del medesimo decreto legislativo, limitatamente ai sistemi informativi e di rete diversi da quelli inseriti nell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui all'articolo 1, comma 2, lettera* b)*, del presente decreto. L'Agenzia per la cybersicurezza nazionale, sentito il tavolo interministeriale per l'attuazione del perimetro di sicurezza nazionale cibernetica, stabilisce con propria determina termini, modalità, specifiche e tempi graduali di implementazione degli obblighi di cui al presente comma.*

9. – 16. (*Omissis*).

17 (*abrogato*).

18. – 19-*ter*. (*Omissis*).».

Note all'art. 44:

— Si riporta il testo dell'articolo 1, commi da 512 a 520, della legge 28 dicembre 2015, n. 208 (Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato, legge di stabilità 2016), pubblicata nella *Gazzetta Ufficiale* 30 dicembre 2015, n. 302:

«512. Al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività, fermi restando gli obblighi di acquisizione centralizzata previsti per i beni e servizi dalla normativa vigente, le amministrazioni pubbliche e le società inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1 della legge 31 dicembre 2009, n. 196, provvedono ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip Spa o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti. Le regioni sono autorizzate ad assumere personale strettamente necessario ad assicurare la piena funzionalità dei soggetti aggregatori di cui all'articolo 9 del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89, in deroga ai vincoli assunzionali previsti dalla normativa vigente, nei limiti del finanziamento derivante dal Fondo di cui al comma 9 del medesimo articolo 9 del decreto-legge n. 66 del 2014.

513. L'Agenzia per l'Italia digitale (Agid) predispone il Piano triennale per l'informatica nella pubblica amministrazione che è approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato. Il Piano contiene, per ciascuna amministrazione o categoria di amministrazioni, l'elenco dei beni e servizi informatici e di connettività e dei relativi costi, suddivisi in spese da sostenere per innovazione e spese per la gestione corrente, individuando altresì i beni e servizi la cui acquisizione riveste particolare rilevanza strategica.

514. Ai fini di cui al comma 512, Consip SpA o il soggetto aggregatore interessato sentita l'Agid per l'acquisizione dei beni e servizi strategici indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui al comma 513, programma gli acquisti di beni e servizi informatici e di connettività, in coerenza con la domanda aggregata di cui al predetto Piano. Agid, Consip SpA e i soggetti aggregatori, sulla base di analisi delle informazioni in loro possesso relative ai contratti di acquisto di beni e servizi in materia informatica, propongono alle amministrazioni e alle società di cui al comma 512 iniziative e misure, anche organizzative e di processo, volte al contenimento della spesa. Consip SpA e gli altri soggetti aggregatori promuovono l'aggregazione della domanda funzionale all'utilizzo degli strumenti messi a disposizione delle pubbliche amministrazioni su base nazionale, regionale o comune a più amministrazioni.

514-*bis*. Per i beni e servizi la cui acquisizione riveste particolare rilevanza strategica secondo quanto indicato nel Piano triennale di cui al comma 513, le amministrazioni statali, centrali e periferiche, ad esclusione degli istituti e delle scuole di ogni ordine e grado, delle istituzioni educative e delle istituzioni universitarie, nonché gli enti nazionali di previdenza ed assistenza sociale pubblici e le agenzie fiscali di cui al decreto legislativo 30 luglio 1999, n. 300, ricorrono a Consip Spa, nell'ambito del Programma di razionalizzazione degli acquisti della pubblica amministrazione del Ministero dell'economia e delle finanze. A tal fine Consip Spa può supportare i soggetti di cui al periodo precedente nell'individuazione di specifici interventi di semplificazione, innovazione e riduzione dei costi dei processi amministrativi. Per le attività di cui al presente comma è previsto un incremento delle dotazioni destinate al finanziamento del Programma di razionalizzazione degli acquisti della pubblica amministrazione del Ministero dell'economia e delle finanze pari a euro 3.000.000 per l'anno 2017, a euro 7.000.000 per l'anno 2018, a euro 4.300.000 per l'anno 2019 e a euro 1.500.000 annui a decorrere dal 2020.

515. La procedura di cui ai commi 512 e 514 ha un obiettivo di risparmio di spesa annuale, da raggiungere alla fine del triennio 2016-2018, pari al 50 per cento della spesa annuale media per la gestione corrente del solo settore informatico, relativa al triennio 2013-2015, al netto dei canoni per servizi di connettività e della spesa effettuata tramite Consip SpA o i soggetti aggregatori documentata nel Piano triennale di cui al comma 513, compresa quella relativa alle acquisizioni di particolare rilevanza strategica di cui al comma 514-*bis*, nonché tramite la società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133. Sono esclusi dal predetto obiettivo di risparmio gli enti disciplinati dalla legge 9 marzo 1989, n. 88, nonché, per le prestazioni e i servizi erogati alle amministrazioni committenti, la società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, la società di cui all'articolo 10, comma 12, della legge 8 maggio 1998, n. 146, e la Consip SpA, nonché l'amministrazione della giustizia in relazione alle spese di investimento necessarie al completamento dell'informatizzazione del processo civile e penale negli uffici giudiziari. I risparmi derivanti dall'attuazione del presente comma sono utilizzati dalle medesime amministrazioni prioritariamente per investimenti in materia di innovazione tecnologica.

515-*bis*. Al fine di facilitare la partecipazione ai programmi comunitari, le amministrazioni pubbliche di cui al comma 510, possono procedere, al di fuori delle modalità di cui al comma 512 e successivi, per attività di ricerca, istruzione, formazione e culturali a richiedere l'accesso alla rete del GARR in quanto unica rete nazionale della ricerca e facente parte della rete della ricerca Europea GEANT, ai sensi dell'articolo 40, comma 6, della legge 1° agosto 2002, n. 166. I relativi costi non sono inclusi nel computo della spesa annuale informatica. La procedura di affidamento segue le disposizioni del comma 516.

516. Le amministrazioni e le società di cui al comma 512 possono procedere ad approvvigionamenti al di fuori delle modalità di cui ai commi 512 e 514 esclusivamente a seguito di apposita autorizzazione motivata dell'organo di vertice amministrativo, qualora il bene o il servizio non sia disponibile o idoneo al soddisfacimento dello specifico fabbisogno dell'amministrazione ovvero in casi di necessità ed urgenza comunque funzionali ad assicurare la continuità della gestione amministrativa. Gli approvvigionamenti effettuati ai sensi del presente comma sono comunicati all'Autorità nazionale anticorruzione e all'Agid.

517. La mancata osservanza delle disposizioni dei commi da 512 a 516 rileva ai fini della responsabilità disciplinare e per danno erariale.

518. Il comma 3-*quinquies* dell'articolo 4 del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135, è abrogato.

519. Nelle acquisizioni di beni e servizi di cui ai commi da 512 al presente comma, gli organi costituzionali adottano le misure idonee a realizzare le economie previste nella rispettiva autonomia, secondo le modalità stabilite nel proprio ordinamento.

520. Per le finalità di cui al comma 512, al fine di consentire l'interoperabilità dei sistemi informativi degli enti del Servizio sanitario nazionale e garantire omogeneità dei processi di approvvigionamento sul territorio nazionale, con accordo sancito in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, previo parere dell'Agid e della Consip SpA, sono definiti criteri uniformi per gli acquisti di beni e servizi informatici e di connettività da parte degli enti del Servizio sanitario nazionale.».

24G00155

ATTI DEGLI ORGANI COSTITUZIONALI

CAMERA DEI DEPUTATI

Convocazione del Parlamento in seduta comune.

La Camera dei deputati ed il Senato della Repubblica sono convocati, in seduta comune, martedì 8 ottobre 2024, alle ore 12,30 con il seguente

Ordine del giorno:

Votazione per l'elezione di un giudice della Corte costituzionale.

Il Presidente della Camera dei deputati
LORENZO FONTANA

24A05227

DECRETI, DELIBERE E ORDINANZE MINISTERIALI

MINISTERO DELL'AGRICOLTURA, DELLA SOVRANITÀ ALIMENTARE E DELLE FORESTE

DECRETO 6 settembre 2024.

Riconoscimento dell'idoneità al Centro di saggio «Agroservice R&S s.r.l.» ad effettuare prove ufficiali di campo, finalizzate alla produzione di dati di efficacia e alla determinazione dell'entità dei residui di prodotti fitosanitari.

IL DIRETTORE
DEL SERVIZIO FITOSANITARIO CENTRALE

Visto il decreto legislativo 17 marzo 1995, n. 194 che, in attuazione della direttiva 91/414/CEE, disciplina l'immissione in commercio dei prodotti fitosanitari;

Visti in particolare i commi 5, 6, 7 e 8 dell'art. 4 del predetto decreto legislativo n. 194/1995;

Visto il decreto del Ministro della sanità del 28 settembre 1995 che modifica gli allegati II e III del suddetto decreto legislativo n. 194/1995;

Visto il decreto interministeriale 27 novembre 1996 che, in attuazione del citato decreto legislativo n. 194/1995, disciplina i principi delle buone pratiche per l'esecuzione delle prove di campo e definisce i requisiti necessari al riconoscimento ufficiale dell'idoneità a condurre prove di campo finalizzate alla registrazione dei prodotti fitosanitari;

Visto il decreto legislativo 30 luglio 1999, n. 300, di riforma dell'organizzazione di Governo a norma dell'art. 11 della legge 15 marzo 1997, n. 59;

Visto il decreto legislativo 30 marzo 2001, n. 165, recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

Visto l'art. 3 del decreto-legge 11 novembre 2022, n. 173, convertito con modificazioni dalla legge 16 dicembre 2022, n. 204, recante «Disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri» ai sensi del quale il Ministero delle politiche agricole alimentari e forestali assume la denominazione di «Ministero dell'agricoltura, della sovranità alimentare e delle foreste», in particolare il comma 3 che dispone che le denominazioni «Ministro dell'agricoltura, della sovranità alimentare e delle foreste» e «Ministero dell'agricoltura, della sovranità alimentare e delle foreste» sostituiscono, a ogni effetto e ovunque presenti, le denominazioni «Ministro delle politiche agricole alimentari e forestali» e «Ministero delle politiche agricole alimentari e forestali»;

Visto il decreto del Presidente del Consiglio dei ministri 16 ottobre 2023, n. 178, inerente «Regolamento recante la riorganizzazione del Ministero dell'agricoltura, della sovranità alimentare e delle foreste a norma dell'art. 1, comma 2, del decreto-legge 22 aprile 2023, n. 44, convertito, con modificazioni, dalla legge 21 giugno 2023,

n. 74» pubblicato nella *Gazzetta Ufficiale* n. 285 del 6 dicembre 2023;

Visto il decreto del Ministro dell'agricoltura, della sovranità alimentare e delle foreste 31 gennaio 2024, n. 47783, registrato alla Corte dei conti il 23 febbraio 2024, al n. 288, con il quale sono stati individuati gli uffici dirigenziali non generali e le relative competenze;

Vista la direttiva del Ministro dell'agricoltura, della sovranità alimentare e delle foreste prot. n. 45910 del 31 gennaio 2024, registrata alla Corte dei conti in data 23 febbraio 2024, al n. 280, recante gli indirizzi generali sull'attività amministrativa e sulla gestione per il 2024;

Vista l'istanza presentata in data 12 marzo 2024 dal Centro di saggio «Agroservice R&S s.r.l.» con sede operativa in contrada Pappariccotta s.n.c. - 76123 Andria (BT);

Vista la direttiva del Capo Dipartimento della politica agricola comune e dello sviluppo rurale prot. n. 64727 del 9 febbraio 2024, registrata all'UCB in data 7 marzo 2024, al n. 168, per l'attuazione degli obiettivi definiti dal Ministro dell'agricoltura, della sovranità alimentare e delle foreste prot. n. 45910 del 31 gennaio 2024;

Vista la direttiva del direttore generale dello sviluppo rurale n. 108781 del 5 marzo 2024, registrata all'UCB in data 12 aprile 2024 al n. 260, con la quale sono stati attribuiti gli obiettivi ai dirigenti e le risorse finanziarie e umane per la loro realizzazione per l'anno 2024;

Visto il decreto direttoriale prot. n. 0193251 del 30 aprile 2024, con il quale è stato conferito al dott. Bruno Caio Faraglia, dirigente di seconda fascia, l'incarico di direttore dell'ufficio dirigenziale non generale DISR V - Servizio fitosanitario centrale, produzioni vegetali - della Direzione generale dello sviluppo rurale del Dipartimento della politica agricola comune e dello sviluppo rurale;

Visto il verbale n. 0414000 del 5 settembre 2024, relativo alla verifica di conformità effettuata in data 31 agosto 2024 dal gruppo ispettivo nominato con nota n. 0254399 del 6 giugno 2024;

Considerato che il suddetto centro ha dichiarato di possedere i requisiti prescritti dalla normativa vigente, a far data dal 12 marzo 2024, a fronte di apposita documentazione presentata;

Considerato l'esito favorevole della verifica di conformità ad effettuare prove di campo a fini registrativi, finalizzate alla produzione di dati di efficacia e alla determinazione dell'entità dei residui di prodotti fitosanitari, effettuata presso il Centro «Agroservice R&S s.r.l.»;

Decreta:

Art. 1.

1. Il Centro «Agroservice R&S s.r.l.» con sede operativa in contrada Pappariccotta s.n.c. - 76123 Andria (BT), è riconosciuto centro di saggio idoneo ad effettuare prove ufficiali di campo con prodotti fitosanitari volte ad ottenere le seguenti informazioni:

a) individuazione dei prodotti di degradazione e di reazione dei metaboliti in piante o prodotti trattati (allegato II, punto 6.1);

b) valutazione del comportamento dei residui delle sostanze attive e dei suoi metaboliti a partire dall'applicazione fino al momento della raccolta o della commercializzazione dei prodotti immagazzinati (allegato II, punto 6.2);

c) definizione del bilancio generale dei residui delle sostanze attive (allegato II, punto 6.3);

d) prove per la determinazione dei residui di principi attivi nei diversi comparti ambientali;

e) determinazione dei residui in o su prodotti trattati, alimenti per l'uomo o per gli animali (allegato III, punto 8.1);

f) prove di campo ambientali ed ecotossicologiche atte alla valutazione del destino e comportamento nell'ambiente delle sostanze attive e dei suoi metaboliti (allegato II, parte A, punto 8.3);

g) valutazione dei dati sui residui nelle colture successive o di rotazione (allegato III, punto 8.5);

h) individuazione dei tempi di carenza per impieghi in pre o *post*-raccolta (allegato III, punto 8.6).

2. Il riconoscimento di cui al comma 1, riguarda le prove di campo di efficacia e la determinazione dell'entità dei residui di prodotti fitosanitari nei seguenti settori di attività:

a) aree non agricole;

b) colture arboree;

c) colture erbacee;

d) colture forestali;

e) colture ornamentali;

f) colture orticole;

g) concia sementi;

h) conservazione *post*-raccolta;

i) diserbo;

j) entomologia;

k) nematologia;

l) patologia vegetale.

Art. 2.

1. Il mantenimento dell'idoneità di cui all'art. 1 è subordinato alle verifiche periodiche e regolari del possesso dei requisiti prescritti, da parte degli ispettori iscritti nell'apposita lista nazionale di cui all'art. 4, comma 8, del citato decreto legislativo n. 194/1995.

2. Il Centro di saggio «Agroservice R&S s.r.l.» è tenuto a comunicare a questo Ministero l'indicazione precisa delle tipologie delle prove che andrà ad eseguire, nonché la loro localizzazione territoriale.

3. Il citato centro è altresì tenuto a comunicare ogni eventuale variazione che interverrà rispetto a quanto dallo stesso dichiarato nell'istanza di riconoscimento, nonché a quanto previsto dal presente decreto.

Art. 3.

1. Il riconoscimento di idoneità, di cui all'art. 1 del presente decreto, ha validità a partire dalla data di ispezione, effettuata il 31 agosto 2024, fino al giorno 31 dicembre 2026.

2. Il Centro di saggio «Agroservice R&S s.r.l.» qualora intenda confermare o variare gli ambiti operativi di cui al presente decreto, potrà inoltrare apposita istanza, corredata dalla relativa documentazione comprovante il possesso dei requisiti richiesti, entro e non oltre il mese di febbraio 2026.

Il presente decreto, ai sensi dell'art. 13 del decreto legislativo n. 196/2003, sarà oggetto di pubblicazione in ottemperanza agli obblighi di legge previsti dal decreto legislativo n. 33/2013 e pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 6 settembre 2024

Il direttore: FARAGLIA

24A05071

DECRETO 6 settembre 2024.

Riconoscimento dell'idoneità al Centro di saggio «Bayer CropScience s.r.l.» ad effettuare prove ufficiali di campo, finalizzate alla produzione di dati di efficacia e alla determinazione dell'entità dei residui di prodotti fitosanitari.

IL DIRETTORE
DEL SERVIZIO FITOSANITARIO CENTRALE

Visto il decreto legislativo 17 marzo 1995, n. 194 che, in attuazione della direttiva 91/414/CEE, disciplina l'immissione in commercio dei prodotti fitosanitari;

Visti in particolare i commi 5, 6, 7 e 8 dell'art. 4 del predetto decreto legislativo n. 194/1995;

Visto il decreto del Ministro della sanità del 28 settembre 1995 che modifica gli allegati II e III del suddetto decreto legislativo n. 194/1995;

Visto il decreto interministeriale 27 novembre 1996 che, in attuazione del citato decreto legislativo n. 194/1995, disciplina i principi delle buone pratiche per l'esecuzione delle prove di campo e definisce i requisiti necessari al riconoscimento ufficiale dell'idoneità a condurre prove di campo finalizzate alla registrazione dei prodotti fitosanitari;

Visto il decreto legislativo 30 luglio 1999, n. 300, di riforma dell'organizzazione di Governo a norma dell'art. 11 della legge 15 marzo 1997, n. 59;

Visto il decreto legislativo 30 marzo 2001, n. 165, recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

Visto l'art. 3 del decreto-legge 11 novembre 2022, n. 173, convertito con modificazioni dalla legge 16 dicembre 2022, n. 204, recante «Disposizioni urgenti in materia di riordino delle attribuzioni dei Ministeri» ai sensi del quale il Ministero delle politiche agricole alimentari e forestali assume la denominazione di «Ministero dell'agricoltura, della sovranità alimentare e delle foreste», in particolare il comma 3 che dispone che le denominazioni «Ministro dell'agricoltura, della sovranità alimentare e delle foreste» e «Ministero dell'agricoltura, della sovranità alimentare e delle foreste» sostituiscono, a ogni effetto e ovunque presenti, le denominazioni «Ministro delle politiche agricole alimentari e forestali» e «Ministero delle politiche agricole alimentari e forestali»;

Visto il decreto del Presidente del Consiglio dei ministri 16 ottobre 2023, n. 178, inerente «Regolamento recante la riorganizzazione del Ministero dell'agricoltura, della sovranità alimentare e delle foreste a norma dell'art. 1, comma 2, del decreto-legge 22 aprile 2023, n. 44, convertito, con modificazioni, dalla legge 21 giugno 2023, n. 74» pubblicato nella *Gazzetta Ufficiale* n. 285 del 6 dicembre 2023;

Visto il decreto del Ministro dell'agricoltura, della sovranità alimentare e delle foreste 31 gennaio 2024, n. 47783, registrato alla Corte dei conti il 23 febbraio 2024, al n. 288, con il quale sono stati individuati gli uffici dirigenziali non generali e le relative competenze;

Vista la direttiva del Ministro dell'agricoltura, della sovranità alimentare e delle foreste prot. n. 45910 del 31 gennaio 2024, registrata alla Corte dei conti in data 23 febbraio 2024, al n. 280, recante gli indirizzi generali sull'attività amministrativa e sulla gestione per il 2024;

Vista l'istanza presentata in data 18 marzo 2024 dal Centro di saggio «Bayer CropScience s.r.l.» con sede operativa in via Aurelia km 36 - 00055 Ladispoli (RM);

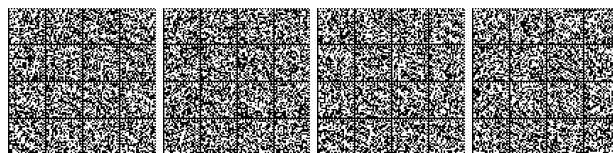
Vista la direttiva del Capo Dipartimento della politica agricola comune e dello sviluppo rurale prot. n. 64727 del 9 febbraio 2024, registrata all'UCB in data 7 marzo 2024, al n. 168, per l'attuazione degli obiettivi definiti dal Ministro dell'agricoltura, della sovranità alimentare e delle foreste prot. n. 45910 del 31 gennaio 2024;

Vista la direttiva del direttore generale dello sviluppo rurale n. 108781 del 5 marzo 2024, registrata all'UCB in data 12 aprile 2024 al n. 260, con la quale sono stati attribuiti gli obiettivi ai dirigenti e le risorse finanziarie e umane per la loro realizzazione per l'anno 2024;

Visto il decreto direttoriale prot. n. 0193251 del 30 aprile 2024, con il quale è stato conferito al dott. Bruno Caio Faraglia, dirigente di seconda fascia, l'incarico di direttore dell'ufficio dirigenziale non generale DISR V - Servizio fitosanitario centrale, produzioni vegetali - della Direzione generale dello sviluppo rurale del Dipartimento della politica agricola comune e dello sviluppo rurale;

Visto il verbale n. 0349807 del 1° agosto 2024, relativo alla verifica di conformità effettuata in data 18 luglio 2024 dal gruppo ispettivo nominato con nota n. 0255594 del 7 luglio 2024;

Considerato che il suddetto centro ha dichiarato di possedere i requisiti prescritti dalla normativa vigente, a far data dal 18 marzo 2024, a fronte di apposita documentazione presentata;

Considerato l'esito favorevole della verifica di conformità ad effettuare prove di campo a fini registrativi, finalizzate alla produzione di dati di efficacia e alla determinazione dell'entità dei residui di prodotti fitosanitari, effettuata presso il Centro «Bayer CropScience s.r.l.»;

Decreta:

Art. 1.

1. Il Centro «Bayer CropScience s.r.l.» con sede operativa in via Aurelia km 36 - 00055 Ladispoli (RM), è riconosciuto centro di saggio idoneo ad effettuare prove ufficiali di campo con prodotti fitosanitari volte ad ottenere le seguenti informazioni:

a) efficacia dei prodotti fitosanitari (di cui all'allegato III, punto 6.2 del decreto legislativo n. 194/1995);

b) dati sulla comparsa o eventuale sviluppo di resistenza (di cui all'allegato III, punto 6.3 del decreto legislativo n. 194/1995);

c) incidenza sulla resa quantitativa e/o qualitativa (di cui all'allegato III, punto 6.4 del decreto legislativo n. 194/1995);

d) fitotossicità nei confronti delle piante e prodotti vegetali bersaglio (di cui all'allegato III, punto 6.5 del decreto legislativo n. 194/1995);

e) osservazioni riguardanti gli effetti collaterali indesiderabili (di cui all'allegato III, punto 6.6 del decreto legislativo n. 194/1995);

f) metabolismo, distribuzione ed espressione del residuo nei vegetali o nel bestiame (di cui al punto 8.1 del regolamento CE n. 545/2011);

g) sperimentazione sui residui (di cui al punto 8.2 del regolamento CE n. 545/2011);

h) definizione del bilancio generale dei residui delle sostanze attive (di cui all'allegato II, punto 6.3 del decreto legislativo n. 194/1995 e punto 8.6 del regolamento CE n. 545/2011);

i) effetti della trasformazione industriale e/o dei preparati domestici (di cui al punto 8.4 del regolamento CE n. 545/2011);

j) residui in colture successive (di cui al punto 8.5 del regolamento CE n. 545/2011);

k) livelli massimi di residui proposti (LMR) e definizione di residuo (di cui al punto 8.6 del regolamento CE n. 545/2011);

l) intervalli pre-raccolta proposti per gli usi previsti, o periodi di sospensione dell'applicazione o periodi di magazzinaggio nel caso di utilizzi *post*-raccolta residuo (di cui al punto 8.7 del regolamento CE n. 545/2011);

m) destino e comportamento nell'ambiente (di cui al punto 9 del regolamento CE n. 545/2011).

2. Il riconoscimento di cui al comma 1, riguarda le prove di campo di efficacia e la determinazione dell'entità dei residui di prodotti fitosanitari nei seguenti settori di attività:

a) aree acquatiche;

b) aree non agricole;

c) colture arboree;

d) colture erbacee;

e) colture forestali;

f) colture medicinali ed aromatiche;

g) colture ornamentali;

h) colture orticole;

i) concia sementi;

j) conservazione *post*-raccolta;

k) diserbo;

l) entomologia;

m) nematologia;

n) patologia vegetale;

o) zoologia agraria;

p) vertebrati dannosi;

q) regolatori di crescita.

Art. 2.

1. Il mantenimento dell'idoneità di cui all'art. 1 è subordinato alle verifiche periodiche e regolari del possesso dei requisiti prescritti, da parte degli ispettori iscritti nell'apposita lista nazionale di cui all'art. 4, comma 8, del citato decreto legislativo n. 194/1995.

2. Il Centro di saggio «Bayer CropScience s.r.l.» è tenuto a comunicare a questo Ministero l'indicazione precisa delle tipologie delle prove che andrà ad eseguire, nonché la loro localizzazione territoriale.

3. Il citato centro è altresì tenuto a comunicare ogni eventuale variazione che interverrà rispetto a quanto dallo stesso dichiarato nell'istanza di riconoscimento, nonché a quanto previsto dal presente decreto.

Art. 3.

1. Il riconoscimento di idoneità, di cui all'art. 1 del presente decreto, ha validità a partire dalla data di ispezione, effettuata il 18 luglio 2024, fino al giorno 31 dicembre 2026.

2. Il Centro di saggio «Bayer CropScience s.r.l.» qualora intenda confermare o variare gli ambiti operativi di cui al presente decreto, potrà inoltrare apposita istanza, corredata dalla relativa documentazione comprovante il possesso dei requisiti richiesti, entro e non oltre il mese di febbraio 2026.

Il presente decreto, ai sensi dell'art. 13 del decreto legislativo n. 196/2003, sarà oggetto di pubblicazione in ottemperanza agli obblighi di legge previsti dal decreto legislativo n. 33/2013 e pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 6 settembre 2024

Il direttore: FARAGLIA

24A05072

MINISTERO DELL'ECONOMIA E DELLE FINANZE

DECRETO 26 settembre 2024.

Emissione dei buoni ordinari del Tesoro a 182 giorni, prima e seconda *tranche*.

IL DIRETTORE GENERALE DEL TESORO

Visto il regio decreto n. 2440 del 18 novembre 1923, concernente disposizioni sull'amministrazione del patrimonio e sulla contabilità generale dello Stato, e in particolare l'articolo 71;

Visto l'articolo 548 del «Regolamento per l'amministrazione del patrimonio e per la contabilità generale dello Stato» (di seguito «Regolamento»), approvato con il regio decreto n. 827 del 23 maggio 1924, così come modificato dall'articolo 1 del decreto del Presidente della Repubblica del 21 aprile 1961, n. 470;

Visto il decreto del Presidente della Repubblica 30 dicembre 2003, n. 398, e successive modifiche, con il quale è stato approvato il «Testo unico delle disposizioni legislative e regolamentari in materia di debito pubblico», (di seguito «Testo unico») e in particolare l'articolo 3, ove si prevede che il Ministro dell'economia e delle finanze è autorizzato, in ogni anno finanziario, ad emanare decreti cornice che consentano, fra l'altro, al Tesoro di effettuare operazioni di indebitamento sul mercato interno o estero nelle forme di prodotti e strumenti finanziari a breve, medio e lungo termine, indicandone l'ammontare nominale, il tasso di interesse o i criteri per la sua determinazione, la durata, l'importo minimo sottoscrivibile, il sistema di collocamento ed ogni altra caratteristica e modalità;

Visto il decreto ministeriale n. 5048315 del 15 dicembre 2023, emanato in attuazione dell'articolo 3 del «Testo unico» (di seguito «decreto cornice»), ove si definiscono per l'anno finanziario 2024 gli obiettivi, i limiti e le modalità cui il Dipartimento del Tesoro dovrà attenersi nell'effettuare le operazioni finanziarie di cui al medesimo articolo prevedendo che le operazioni stesse vengano disposte dal direttore generale del Tesoro o, per sua delega, dal direttore della Direzione II del Dipartimento medesimo e che, in caso di assenza o impedimento di quest'ultimo, le operazioni predette possano essere disposte dal medesimo direttore generale del Tesoro, anche in presenza di delega continuativa;

Visto il decreto del Ministro dell'economia e delle finanze n. 216 del 22 dicembre 2009 ed in particolare l'articolo 23 relativo agli operatori «Specialisti in titoli di Stato italiani» (di seguito «Specialisti»);

Visto il decreto dirigenziale n. 993039 dell'11 novembre 2011 (Decreto dirigenziale specialisti), concernente la «Selezione e la valutazione degli specialisti in titoli di Stato» e successive modifiche e integrazioni;

Visto il decreto legislativo del 1° aprile 1996, n. 239, e successive modifiche e integrazioni;

Visto il decreto legislativo del 21 novembre 1997, n. 461, e successive modifiche e integrazioni, recante disposizioni di riordino della disciplina dei redditi di capitale e dei redditi diversi;

Visti gli articoli 4 e 11 del testo unico, riguardanti la dematerializzazione dei titoli di Stato;

Visti gli articoli 24 e seguenti del testo unico, in materia di gestione accentrata dei titoli di Stato;

Visto il decreto ministeriale del 17 aprile 2000, n. 143, con cui è stato adottato il regolamento concernente la disciplina della gestione accentrata dei titoli di Stato;

Visto il decreto direttoriale del 23 agosto 2000, con cui è stato affidato alla Monte Titoli S.p.a. (oggi *Euronext Securities Milan*) il servizio di gestione accentrata dei titoli di Stato;

Visto l'articolo 17 del testo unico, relativo all'ammissibilità del servizio di riproduzione in fac-simile nella partecipazione alle aste dei titoli di Stato;

Visto il decreto ministeriale n. 3088 del 15 gennaio 2015, recante norme per la trasparenza nelle operazioni di collocamento dei titoli di Stato;

Visto il regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n. 236/2012, come successivamente modificato dal regolamento (UE) n. 2023/2845 del Parlamento europeo e del Consiglio del 13 dicembre 2023 per quanto riguarda la disciplina di regolamento, la prestazione di servizi transfrontalieri, la cooperazione in materia di vigilanza, la prestazione di servizi accessori di tipo bancario e i requisiti per i depositari centrali di titoli di paesi terzi, e come integrato dal regolamento delegato (UE) n. 2017/389 della Commissione dell'11 novembre 2016 per quanto riguarda i parametri per il calcolo delle penali pecuniarie per mancati regolamenti e le operazioni dei depositari centrali di titoli (CSD) negli Stati membri ospitanti e dal regolamento delegato (UE) n. 2018/1229 della Commissione del 25 maggio 2018 per quanto riguarda le norme tecniche di regolamentazione sulla disciplina del regolamento, come modificato dal regolamento delegato (UE) n. 2021/70 della Commissione del 23 ottobre 2020 con riferimento all'entrata in vigore dello stesso, dal regolamento delegato (UE) n. 2022/1930 della Commissione del 6 luglio 2022 per quanto riguarda la data di applicazione delle disposizioni relative alla procedura di acquisto forzoso e, da ultimo, dal regolamento delegato (UE) n. 2023/1626 della Commissione del 19 aprile 2023 per quanto riguarda il meccanismo di penalizzazione per i mancati regolamenti relativi alle operazioni compensate che le controparti centrali presentano a fini di regolamento;

Visto il decreto ministeriale n. 12953 del 17 febbraio 2023, concernente le «Disposizioni contabili in caso di ritardo nel regolamento delle operazioni di emissione, concambio e riacquisto di titoli di Stato, nonché nelle operazioni di pronti contro termine svolte dal Ministero dell'economia e delle finanze»;

Vista la legge 30 dicembre 2023, n. 213, recante il «bilancio di previsione dello Stato per l'anno finanziario 2024 e il bilancio pluriennale per il triennio 2024-2026», ed in particolare l'articolo 3, comma 2, con cui è stato stabilito il limite massimo di emissione dei prestiti pubblici per l'anno stesso;

Viste le linee guida della gestione del debito pubblico 2024;

Vista la determinazione n. 101204 del 23 novembre 2023, con la quale il direttore generale del Tesoro ha conferito a decorrere dal 1° gennaio 2024 la delega al dirigente generale Capo della Direzione II in relazione alle attribuzioni in materia di debito pubblico, di cui al menzionato art. 3 del decreto del Presidente della Repubblica n. 398/2003, al fine di assicurare la continuità e la tempestività dell'azione amministrativa;

Ravvisata l'esigenza di svolgere le aste dei buoni ordinari del Tesoro con richieste degli operatori ammessi a partecipare espresse in termini di rendimento, anziché di prezzo, secondo la prassi prevalente sui mercati monetari dell'area euro;

Considerato che l'importo delle emissioni disposte a tutto il 23 settembre 2024 ammonta, al netto dei rimborsi di prestiti pubblici già effettuati, a 97.284 milioni di euro;

Decreta:

Art. 1.

Ai sensi e per gli effetti dell'articolo 3 del testo unico nonché del decreto cornice, e in deroga all'articolo 548 del regolamento, è disposta per il 30 settembre 2024 l'emissione di una prima *tranche* dei buoni ordinari del Tesoro (appresso denominati *BOT)*, a centottantadue giorni con scadenza 31 marzo 2025, fino al limite massimo in valore nominale di 7.000 milioni di euro.

Per la presente emissione è possibile effettuare riaperture in *tranche*.

Al termine della procedura di assegnazione, è altresì disposta l'emissione di un collocamento supplementare dei BOT di cui al presente decreto.

Art. 2.

Sono escluse automaticamente dall'asta le richieste effettuate a rendimenti inferiori al «rendimento minimo accoglibile», determinato in base alle seguenti modalità:

a) nel caso di domanda totale superiore all'offerta, si determina il rendimento medio ponderato delle richieste che, ordinate a partire dal rendimento più basso, costituiscono la seconda metà dell'importo nominale in emissione; nel caso di domanda totale inferiore all'offerta, si determina il rendimento medio ponderato delle richieste che, ordinate a partire dal rendimento più basso, costituiscono la seconda metà dell'importo domandato;

b) si individua il rendimento minimo accoglibile, corrispondente al rendimento medio ponderato di cui al punto *a)* decurtato di 50 punti base (1 punto percentuale = 100 punti base).

In caso di esclusione ai sensi del primo comma del presente articolo, il rendimento medio ponderato di aggiudicazione si determina sottraendo dalla quantità totale offerta dall'emittente una quantità pari a quella esclusa. Le richieste escluse sono assegnate ad un rendimento pari al maggiore tra il rendimento ottenuto sottraendo 10 punti base al rendimento minimo accolto nell'asta e il rendimento minimo accoglibile.

Art. 3.

Sono escluse dall'assegnazione le richieste effettuate a rendimenti superiori di oltre 100 punti base rispetto al rendimento medio ponderato delle richieste che, ordinate partendo dal rendimento più basso, costituiscono la metà dell'ammontare complessivo di quelle pervenute. Nel caso in cui tale ammontare sia superiore alla *tranche* offerta, il rendimento medio ponderato viene calcolato sulla base dell'importo complessivo delle richieste, ordinate in modo crescente rispetto al rendimento e pari alla metà della *tranche* offerta.

Sono escluse dal calcolo del rendimento medio ponderato di cui al presente articolo le richieste escluse ai sensi dell'articolo 2 del presente decreto.

Art. 4.

Espletate le operazioni di asta, con successivo decreto vengono indicati il rendimento minimo accoglibile e il rendimento massimo accoglibile - derivanti dai meccanismi di cui agli articoli 2 e 3 del presente decreto - e il rendimento medio ponderato di aggiudicazione, nonché il corrispondente prezzo medio ponderato.

In caso di emissioni di *tranche* successive alla prima, il decreto di cui al comma precedente riporterà altresì il prezzo medio ponderato determinato ai fini fiscali, ai sensi dell'articolo 17 del presente decreto.

Art. 5.

I BOT sono sottoscritti per un importo minimo di 1.000 euro e gli importi sottoscritti sono rappresentati da iscrizioni contabili a favore degli aventi diritto.

La Banca d'Italia provvede a inserire in via automatica le partite dei BOT sottoscritti in asta da regolare nel servizio di compensazione e liquidazione avente a oggetto strumenti finanziari con valuta pari a quella di regolamento. L'operatore partecipante all'asta, al fine di regolare i BOT assegnati, può avvalersi di un altro intermediario da comunicare alla Banca d'Italia, in base alla normativa e alle modalità dalla stessa stabilite.

Sulla base delle assegnazioni, gli intermediari aggiudicatari accreditano i relativi importi sui conti intrattenuti con i sottoscrittori.

Art. 6.

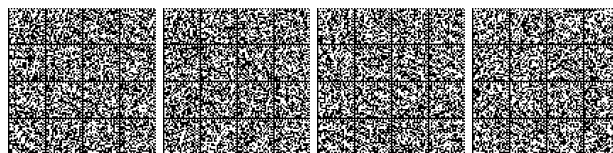
In deroga al disposto del sopramenzionato articolo 548 del regolamento, la durata dei BOT può essere espressa in «giorni».

Il computo dei giorni ai fini della determinazione della scadenza decorre dal giorno successivo a quello del regolamento dei BOT.

Art. 7.

Possono partecipare all'asta gli operatori specialisti nonché gli aspiranti specialisti.

Sia gli specialisti che gli aspiranti partecipano in proprio e per conto terzi.

La Banca d'Italia è autorizzata a stipulare apposite convenzioni con gli operatori specialisti e con gli operatori notificati dal Ministero dell'economia e delle finanze che intendano avanzare

domanda di iscrizione nell'elenco specialisti, per regolare la partecipazione alle aste tramite la rete nazionale interbancaria.

Alla Banca d'Italia, quale gerente il servizio di tesoreria provinciale dello Stato, viene affidata l'esecuzione delle operazioni.

Art. 8.

Le richieste di acquisto da parte degli operatori ammessi a partecipare alle aste devono essere formulate in termini di rendimento, che può assumere valori positivi, nulli o negativi. Tali rendimenti sono da considerare lordi ed espressi in regime di capitalizzazione semplice riferita all'anno di trecentosessanta giorni.

Le richieste degli operatori devono essere inviate tramite la rete nazionale interbancaria e devono contenere sia l'indicazione dell'importo dei BOT che si intende sottoscrivere sia il relativo rendimento. Non sono ammesse all'asta richieste senza indicazione del rendimento.

I rendimenti indicati dagli operatori in sede d'asta, espressi in termini percentuali, possono variare di un millesimo di punto percentuale o multiplo di tale cifra. Eventuali variazioni di importo diverso vengono arrotondate per difetto.

L'importo di ciascuna richiesta non può essere inferiore a 1.500.000 euro di capitale nominale.

Le richieste di ciascun operatore che indichino un importo che superi, anche come somma complessiva di esse, quello offerto dal Tesoro sono prese in considerazione a partire da quella con il rendimento più basso e fino a concorrenza dell'importo offerto, salvo quanto stabilito agli articoli 2 e 3 del presente decreto.

Le richieste di importo non multiplo dell'importo minimo sottoscrivibile di cui all'articolo 5 vengono arrotondate per difetto.

Eventuali offerte che presentino l'indicazione di titoli di scambio da versare in regolamento dei titoli in emissione non verranno prese in considerazione.

Art. 9.

Le richieste di ogni singolo operatore, da indirizzare alla Banca d'Italia, devono essere trasmesse utilizzando la rete nazionale interbancaria secondo le modalità tecniche stabilite dalla Banca d'Italia medesima.

Al fine di garantire l'integrità e la riservatezza dei dati trasmessi attraverso la rete nazionale interbancaria, sono scambiate chiavi bilaterali di autenticazione e crittografia tra operatori e Banca d'Italia.

Nell'impossibilità di immettere messaggi in rete a causa di malfunzionamento delle apparecchiature, le richieste di partecipazione all'asta debbono essere inviate mediante modulo da trasmettere alla Banca d'Italia, secondo quanto previsto dalle convenzioni di cui all'articolo 7, comma 3, del presente decreto.

Art. 10.

Le richieste di acquisto dovranno pervenire alla Banca d'Italia entro e non oltre le ore 11,00 del giorno 26 settembre 2024. Le richieste non pervenute entro tale termine non verranno prese in considerazione.

Eventuali richieste sostitutive di quelle corrispondenti già pervenute vengono prese in considerazione soltanto se giunte entro il termine di cui sopra.

Le richieste non possono essere più ritirate dopo il termine suddetto.

Art. 11.

Le operazioni d'asta vengono eseguite dalla Banca d'Italia, dopo la scadenza del termine di cui all'articolo precedente, in presenza di un rappresentante della Banca medesima e con l'intervento, anche tramite sistemi di comunicazione telematica, di un rappresentante del Ministero dell'economia e delle finanze, che ha funzioni di ufficiale rogante e redige apposito verbale nel quale devono essere evidenziati, per ciascuna tranche, i rendimenti di aggiudicazione e l'ammontare dei relativi interessi passivi o attivi, determinati dalla differenza tra 100 e i corrispondenti prezzi di aggiudicazione.

In caso di eventi straordinari la Banca d'Italia ed il Ministero dell'economia e delle finanze, in deroga a quanto previsto dal comma precedente, ciascuno per le rispettive competenze, possono scegliere di svolgere le operazioni d'asta, relative al titolo oggetto della presente emissione, da remoto mediante l'ausilio di strumenti informatici, sulla base di modalità concordate dalle due istituzioni.

Art. 12.

Le sezioni di Tesoreria dello Stato sono autorizzate a contabilizzare l'importo degli interessi in apposito unico documento riassuntivo per ciascuna *tranche* emessa e rilasciano – nello stesso giorno fissato per l'emissione dei BOT dal presente decreto – quietanze d'entrata per l'importo nominale emesso.

La spesa per gli interessi passivi graverà sul capitolo 2215 (unità di voto 21.1) dello stato di previsione della spesa del Ministero dell'economia e delle finanze dell'esercizio finanziario 2025 o a quelli corrispondenti per il medesimo anno.

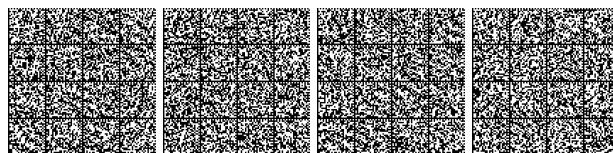
L'entrata relativa agli interessi attivi verrà imputata al Capo X, capitolo 3240, articolo 3 (unità di voto 2.1.93), con valuta pari al giorno di regolamento dei titoli indicato nell'articolo 1, comma 1 del presente decreto. A fronte di tale versamento, la competente sezione di Tesoreria dello Stato rilascerà apposita quietanza di entrata.

Art. 13.

L'assegnazione dei BOT è effettuata al rendimento rispettivamente indicato da ciascun operatore partecipante all'asta, che può presentare fino a cinque richieste ciascuna a un rendimento diverso.

Art. 14.

L'aggiudicazione dei BOT viene effettuata seguendo l'ordine crescente dei rendimenti offerti dagli operatori, fino a concorrenza dell'importo offerto, salvo quanto specificato agli articoli 2 e 3 del presente decreto.

Nel caso in cui le richieste formulate al rendimento massimo accolto non possano essere totalmente soddisfatte, si procede al riparto *pro-quota*.

Le richieste risultate aggiudicate vengono regolate ai prezzi corrispondenti ai rendimenti indicati dagli operatori.

Art. 15.

Ultimate le operazioni di assegnazione, ha inizio il collocamento supplementare di detti titoli, di cui all'articolo 1 del presente decreto, per un importo pari al 10% dell'ammontare nominale offerto nell'asta ordinaria.

Tale *tranche* è riservata ai soli specialisti che hanno partecipato all'asta della *tranche* ordinaria con almeno una richiesta effettuata a un rendimento non superiore al rendimento massimo accoglibile di cui all'articolo 3 del presente decreto. Questi possono partecipare al collocamento supplementare inoltrando le domande di sottoscrizione fino alle ore 15,30 del giorno 27 settembre 2024.

Le offerte non pervenute entro tale termine non verranno prese in considerazione.

Il collocamento supplementare ha luogo al rendimento medio ponderato di aggiudicazione dell'asta della *tranche* ordinaria; eventuali richieste formulate ad un rendimento diverso vengono aggiudicate al descritto rendimento medio ponderato.

Ai fini dell'assegnazione valgono, in quanto applicabili, le disposizioni di cui agli articoli 5 e 11. La richiesta di ciascuno specialista dovrà essere presentata secondo le modalità degli articoli 9 e 10 e deve contenere l'indicazione dell'importo dei titoli che si intende sottoscrivere.

Ciascuna richiesta non può essere inferiore ad 1.500.000 euro; eventuali richieste di importo inferiore non vengono prese in considerazione.

Ciascuna richiesta non può superare l'intero importo offerto nel collocamento supplementare; eventuali richieste di ammontare superiore sono accettate fino al limite dell'importo offerto nel collocamento supplementare stesso.

Le richieste di importo non multiplo dell'importo minimo sottoscrivibile di cui all'articolo 5 vengono arrotondate per difetto.

Eventuali offerte che presentino l'indicazione di titoli di scambio da versare in regolamento dei titoli in emissione non verranno prese in considerazione.

Art. 16.

L'importo spettante di diritto a ciascuno specialista nel collocamento supplementare è così determinato:

a) per un importo pari al 5% dell'ammontare nominale offerto nell'asta ordinaria, è pari al rapporto fra il valore dei titoli di cui lo specialista è risultato aggiudicatario nelle ultime tre aste ordinarie dei BOT semestrali, ivi compresa quella ordinaria immediatamente precedente alla riapertura stessa, e il totale assegnato nelle medesime aste agli stessi specialisti ammessi a partecipare al collocamento supplementare; non concorrono alla determinazione dell'importo spettante a ciascuno specialista gli importi assegnati secondo le modalità di cui all'articolo 2 del presente decreto;

b) per un importo ulteriore pari al 5% dell'ammontare nominale offerto nell'asta ordinaria, è attribuito in base alla valutazione, effettuata dal Tesoro, della performance relativa agli specialisti medesimi, rilevata trimestralmente sulle sedi di negoziazione all'ingrosso selezionate ai sensi dell'articolo 23, commi 10, 11, 13 e 14, del decreto del Ministro dell'economia e delle finanze del 22 dicembre 2009, n. 216, citato nelle premesse; tale valutazione viene comunicata alla Banca d'Italia e agli specialisti stessi.

Le richieste sono soddisfatte assegnando prioritariamente a ciascuno specialista il minore tra l'importo richiesto e quello spettante di diritto. Qualora uno o più specialisti dovessero presentare richieste inferiori a quelle loro spettanti di diritto, ovvero non abbiano effettuato alcuna richiesta, la differenza viene assegnata agli operatori che abbiano presentato richieste superiori a quelle spettanti di diritto. L'assegnazione viene effettuata in base alle quote di cui alle precedenti lettere *a)* e *b)*.

Il regolamento dei titoli sottoscritti nel collocamento supplementare viene effettuato dagli operatori assegnatari nello stesso giorno di regolamento dei titoli assegnati nell'asta ordinaria indicato nell'articolo 1, comma 1 del presente decreto.

Art. 17.

L'ammontare degli interessi derivanti dai BOT è corrisposto anticipatamente ed è determinato, ai soli fini fiscali, con riferimento al prezzo medio ponderato - espresso con arrotondamento al terzo decimale - corrispondente al rendimento medio ponderato della prima *tranche*.

Ferme restando le disposizioni vigenti relative alle esenzioni fiscali in materia di debito pubblico, ai BOT emessi con il presente decreto si applicano le disposizioni di cui al decreto legislativo del 1° aprile 1996, n. 239, e successive modifiche e integrazioni, e al decreto legislativo del 21 novembre 1997, n. 461 e successive modifiche e integrazioni.

Il presente decreto sarà pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 26 settembre 2024

p. Il direttore generale del Tesoro: IACOVONI

24A05110

DECRETO 27 settembre 2024.

Riapertura delle operazioni di sottoscrizione dei buoni del Tesoro poliennali 3,00%, con godimento 1° febbraio 2019 e scadenza 1° agosto 2029, diciassettesima e diciottesima *tranche.*

IL DIRETTORE GENERALE
DEL TESORO

Visto il decreto del Presidente della Repubblica 30 dicembre 2003, n. 398, e successive modifiche, con il quale è stato approvato il «Testo unico delle disposizioni legislative e regolamentari in materia di debito pubblico» (di seguito «Testo unico»), ed in particolare l'art. 3, ove si prevede che il Ministro dell'economia e delle finanze è autorizzato, in ogni anno finanziario, ad emanare decreti cornice che consentano, fra l'altro, al Tesoro di effettuare operazioni di indebitamento sul mercato interno o estero nelle forme di prodotti e strumenti finanziari a breve, me-

dio e lungo termine, indicandone l'ammontare nominale, il tasso di interesse o i criteri per la sua determinazione, la durata, l'importo minimo sottoscrivibile, il sistema di collocamento ed ogni altra caratteristica e modalità;

Visto il decreto n. 101633 del 19 dicembre 2022 (di seguito «decreto di massima) e successive modifiche ed integrazioni con il quale sono state stabilite in maniera continuativa le caratteristiche e la modalità di emissione dei titoli di Stato a medio e lungo termine da collocare tramite asta;

Visto il decreto ministeriale n. 5048315 del 15 dicembre 2023, emanato in attuazione dell'art. 3 del «Testo unico» (di seguito «decreto cornice»), ove si definiscono per l'anno finanziario 2024 gli obiettivi, i limiti e le modalità cui il Dipartimento del tesoro dovrà attenersi nell'effettuare le operazioni finanziarie di cui al medesimo articolo prevedendo che le operazioni stesse vengano disposte dal direttore generale del Tesoro o, per sua delega, dal direttore della Direzione seconda del Dipartimento medesimo e che, in caso di assenza o impedimento di quest'ultimo, le operazioni predette possano essere disposte dal medesimo direttore generale del Tesoro, anche in presenza di delega continuativa;

Visto il regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n. 236/2012, come successivamente modificato dal regolamento (UE) n. 2023/2845 del Parlamento europeo e del Consiglio del 13 dicembre 2023 per quanto riguarda la disciplina di regolamento, la prestazione di servizi transfrontalieri, la cooperazione in materia di vigilanza, la prestazione di servizi accessori di tipo bancario e i requisiti per i depositari centrali di titoli di paesi terzi, e come integrato dal regolamento delegato (UE) n. 2017/389 della Commissione dell'11 novembre 2016 per quanto riguarda i parametri per il calcolo delle penali pecuniarie per mancati regolamenti e le operazioni dei depositari centrali di titoli (CSD) negli Stati membri ospitanti e dal regolamento delegato (UE) n. 2018/1229 della Commissione del 25 maggio 2018 per quanto riguarda le norme tecniche di regolamentazione sulla disciplina del regolamento, come modificato dal regolamento delegato (UE) n. 2021/70 della Commissione del 23 ottobre 2020 con riferimento all'entrata in vigore dello stesso, dal regolamento delegato (UE) n. 2022/1930 della Commissione del 6 luglio 2022 per quanto riguarda la data di applicazione delle disposizioni relative alla procedura di acquisto forzoso e, da ultimo, dal regolamento delegato (UE) n. 2023/1626 della Commissione del 19 aprile 2023 per quanto riguarda il meccanismo di penalizzazione per i mancati regolamenti relativi alle operazioni compensate che le controparti centrali presentano a fini di regolamento;

Visto il decreto ministeriale n. 12953 del 17 febbraio 2023, concernente le «Disposizioni contabili in caso di ritardo nel regolamento delle operazioni di emissione, concambio e riacquisto di titoli di Stato, nonché nelle operazioni di pronti contro termine svolte dal Ministero dell'economia e delle finanze»;

Visto il decreto ministeriale n. 96718 del 7 dicembre 2012, concernente le «Disposizioni per le operazioni di separazione, negoziazione e ricostituzione delle componenti cedolari, della componente indicizzata all'inflazione e del valore nominale di rimborso dei titoli di Stato *(stripping)*»;

Vista la legge 30 dicembre 2023, n. 213, recante il «bilancio di previsione dello Stato per l'anno finanziario 2024 e il bilancio pluriennale per il triennio 2024-2026», ed in particolare l'art. 3, comma 2, con cui è stato stabilito il limite massimo di emissione dei prestiti pubblici per l'anno stesso;

Considerato che l'importo delle emissioni disposte a tutto il 24 settembre 2024 ammonta, al netto dei rimborsi di prestiti pubblici già effettuati, a 97.284 milioni di euro;

Vista la determinazione n. 101204 del 23 novembre 2023, con la quale il direttore generale del Tesoro ha conferito a decorrere dal 1° gennaio 2024 la delega al dirigente generale Capo della Direzione II in relazione alle attribuzioni in materia di debito pubblico, di cui al menzionato art. 3 del decreto del Presidente della Repubblica n. 398/2003, al fine di assicurare la continuità e la tempestività dell'azione amministrativa;

Visti i propri decreti in data 26 febbraio, 27 marzo, 29 aprile, 29 maggio, 26 giugno e 29 luglio 2019, il decreto del 18 maggio 2021 relativo alla costituzione di titoli per l'operatività pronti contro termine del Ministero dell'economia e delle finanze (REPO), nonché del 16 giugno 2021 e del 13 aprile 2022, con i quali è stata disposta l'emissione delle prime sedici *tranche* dei buoni del Tesoro poliennali 3,00% con godimento 1° febbraio 2019 e scadenza 1° agosto 2029;

Ritenuto opportuno, in relazione alle condizioni di mercato, disporre l'emissione di una diciassettesima *tranche* dei predetti buoni del Tesoro poliennali;

Decreta:

Art. 1.

Ai sensi e per gli effetti dell'art. 3 del «Testo unico» nonché del «decreto cornice», è disposta l'emissione di una diciassettesima *tranche* dei buoni del Tesoro poliennali 3,00%, avente godimento 1° febbraio 2019 e scadenza 1° agosto 2029. L'emissione della predetta *tranche* viene disposta per un ammontare nominale compreso fra un importo minimo di 750 milioni di euro e un importo massimo di 1.000 milioni di euro.

I buoni fruttano l'interesse annuo lordo del 3,00%, pagabile in due semestralità posticipate, il 1° febbraio ed il 1° agosto di ogni anno di durata del prestito.

Le prime undici cedole dei buoni emessi con il presente decreto, essendo pervenute in scadenza, non verranno corrisposte.

Sui buoni medesimi possono essere effettuate operazioni di separazione e ricostituzione delle componenti cedolari dal valore di rimborso del titolo *(«coupon stripping»)*.

Le caratteristiche e le modalità di emissione dei predetti titoli sono quelle definite nel «decreto di massima», che qui si intende interamente richiamato ed a cui si rinvia per quanto non espressamente disposto dal presente decreto.

Art. 2.

Le offerte degli operatori relative alla *tranche* di cui all'art. 1 del presente decreto dovranno pervenire entro le ore 11,00 del giorno 27 settembre 2024, con l'osservanza delle modalità indicate negli articoli 7, 8, 9, 10 e 11 del «decreto di massima».

La provvigione di collocamento, pari a 0,150% del capitale nominale sottoscritto, verrà corrisposta secondo le modalità di cui all'art. 8 del «decreto di massima» indicato nelle premesse.

Art. 3.

Al termine delle operazioni di assegnazione di cui al precedente articolo ha luogo il collocamento della diciottesima *tranche* dei titoli stessi, secondo le modalità indicate negli articoli 12, 13, 14 e 15 del «decreto di massima».

L'importo della *tranche* relativa al titolo oggetto della presente emissione sarà pari al 20 per cento secondo quanto stabilito dall'art. 14, comma 2, del «decreto di massima».

Gli specialisti in titoli di Stato hanno la facoltà di partecipare al collocamento supplementare, inoltrando le domande di sottoscrizione entro le ore 15,30 del giorno 30 settembre 2024.

Art. 4.

Il regolamento dei buoni sottoscritti in asta e nel collocamento supplementare sarà effettuato dagli operatori assegnatari il 1° ottobre 2024, al prezzo di aggiudicazione e con corresponsione di dietimi di interesse lordi per sessantuno giorni. A tal fine la Banca d'Italia provvederà ad inserire, in via automatica, le relative partite nel servizio di compensazione e liquidazione con valuta pari al giorno di regolamento.

In caso di ritardo nel regolamento dei titoli di cui al presente decreto, troveranno applicazione le disposizioni del regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 e del decreto ministeriale n. 12953 del 17 febbraio 2023, citati nelle premesse.

Art. 5.

Il 1° ottobre 2024 la Banca d'Italia provvederà a versare, presso la Sezione di Roma della Tesoreria dello Stato, il ricavo dei buoni assegnati al prezzo di aggiudicazione d'asta unitamente al rateo di interesse del 3,00% annuo lordo, dovuto allo Stato.

La predetta sezione di Tesoreria rilascia, per detti versamenti, separate quietanze di entrata al bilancio dello Stato, con imputazione al Capo X, capitolo 5100, art. 3 (unità di voto parlamentare 4.1.171) per l'importo relativo al ricavo dell'emissione ed al capitolo 3240, art. 3 (unità di voto parlamentare 2.1.93) per quello relativo ai dietimi d'interesse lordi dovuti.

Art. 6.

Gli oneri per interessi relativi agli anni finanziari dal 2025 al 2029, nonché l'onere per il rimborso del capitale relativo all'anno finanziario 2029, faranno carico ai capitoli che verranno iscritti nello stato di previsione della spesa del Ministero dell'economia e delle finanze per gli anni stessi e corrispondenti, rispettivamente, ai capitoli 2214 (unità di voto parlamentare 21.1) e 9502 (unità di voto parlamentare 21.2) dello stato di previsione per l'anno in corso.

L'ammontare della provvigione di collocamento, prevista dall'art. 2 del presente decreto, sarà scritturato, ad ogni cadenza di pagamento trimestrale, dalle sezioni di Tesoreria fra i «pagamenti da regolare» e farà carico al capitolo 2247 (unità di voto parlamentare 21.1; codice gestionale 109) dello stato di previsione della spesa del Ministero dell'economia e delle finanze per l'anno finanziario 2024 o a quello corrispondente per gli anni successivi.

Il presente decreto sarà pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 27 settembre 2024

p. Il direttore generale del Tesoro: IACOVONI

24A05138

DECRETO 27 settembre 2024.

Riapertura delle operazioni di sottoscrizione dei buoni del Tesoro poliennali 3,85%, con godimento 1° agosto 2024 e scadenza 1° febbraio 2035, quinta e sesta *tranche*.

IL DIRETTORE GENERALE DEL TESORO

Visto il decreto del Presidente della Repubblica 30 dicembre 2003, n. 398, e successive modifiche, con il quale è stato approvato il «Testo unico delle disposizioni legislative e regolamentari in materia di debito pubblico» (di seguito «Testo unico»), ed in particolare l'art. 3, ove si prevede che il Ministro dell'economia e delle finanze è autorizzato, in ogni anno finanziario, ad emanare decreti cornice che consentano, fra l'altro, al Tesoro di effettuare operazioni di indebitamento sul mercato interno o estero nelle forme di prodotti e strumenti finanziari a breve, medio e lungo termine, indicandone l'ammontare nominale, il tasso di interesse o i criteri per la sua determinazione, la durata, l'importo minimo sottoscrivibile, il sistema di collocamento ed ogni altra caratteristica e modalità;

Visto il decreto n. 101633 del 19 dicembre 2022 (di seguito «decreto di massima») e successive modifiche ed integrazioni con il quale sono state stabilite in maniera continuativa le caratteristiche e la modalità di emissione dei titoli di Stato a medio e lungo termine da collocare tramite asta;

Visto il decreto ministeriale n. 5048315 del 15 dicembre 2023, emanato in attuazione dell'art. 3 del «Testo unico» (di seguito «decreto cornice»), ove si definiscono per l'anno finanziario 2024 gli obiettivi, i limiti e le modalità cui il Dipartimento del tesoro dovrà attenersi nell'effettuare le operazioni finanziarie di cui al medesimo articolo prevedendo che le operazioni stesse vengano disposte dal direttore generale del Tesoro o, per sua delega, dal direttore della Direzione II del Dipartimento medesimo e che, in caso di assenza o impedimento di quest'ultimo, le operazioni predette possano essere disposte dal mede-

simo direttore generale del tesoro, anche in presenza di delega continuativa;

Visto il regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014, relativo al miglioramento del regolamento titoli nell'Unione europea e ai depositari centrali di titoli e recante modifica delle direttive 98/26/CE e 2014/65/UE e del regolamento (UE) n. 236/2012, come successivamente modificato dal regolamento (UE) n. 2023/2845 del Parlamento europeo e del Consiglio del 13 dicembre 2023 per quanto riguarda la disciplina di regolamento, la prestazione di servizi transfrontalieri, la cooperazione in materia di vigilanza, la prestazione di servizi accessori di tipo bancario e i requisiti per i depositari centrali di titoli di paesi terzi, e come integrato dal regolamento delegato (UE) n. 2017/389 della Commissione dell'11 novembre 2016 per quanto riguarda i parametri per il calcolo delle penali pecuniarie per mancati regolamenti e le operazioni dei depositari centrali di titoli (CSD) negli Stati membri ospitanti e dal regolamento delegato (UE) n. 2018/1229 della Commissione del 25 maggio 2018 per quanto riguarda le norme tecniche di regolamentazione sulla disciplina del regolamento, come modificato dal regolamento delegato (UE) n. 2021/70 della Commissione del 23 ottobre 2020 con riferimento all'entrata in vigore dello stesso, dal regolamento delegato (UE) n. 2022/1930 della Commissione del 6 luglio 2022 per quanto riguarda la data di applicazione delle disposizioni relative alla procedura di acquisto forzoso e, da ultimo, dal regolamento delegato (UE) n. 2023/1626 della Commissione del 19 aprile 2023 per quanto riguarda il meccanismo di penalizzazione per i mancati regolamenti relativi alle operazioni compensate che le controparti centrali presentano a fini di regolamento;

Visto il decreto ministeriale n. 12953 del 17 febbraio 2023, concernente le «Disposizioni contabili in caso di ritardo nel regolamento delle operazioni di emissione, concambio e riacquisto di titoli di Stato, nonché nelle operazioni di pronti contro termine svolte dal Ministero dell'economia e delle finanze»;

Visto il decreto ministeriale n. 96718 del 7 dicembre 2012, concernente le «Disposizioni per le operazioni di separazione, negoziazione e ricostituzione delle componenti cedolari, della componente indicizzata all'inflazione e del valore nominale di rimborso dei titoli di Stato *(stripping)*»;

Vista la legge 30 dicembre 2023, n. 213, recante il «bilancio di previsione dello Stato per l'anno finanziario 2024 e il bilancio pluriennale per il triennio 2024-2026», ed in particolare l'art. 3, comma 2, con cui è stato stabilito il limite massimo di emissione dei prestiti pubblici per l'anno stesso;

Considerato che l'importo delle emissioni disposte a tutto il 24 settembre 2024 ammonta, al netto dei rimborsi di prestiti pubblici già effettuati, a 97.284 milioni di euro;

Vista la determinazione n. 101204 del 23 novembre 2023, con la quale il direttore generale del Tesoro ha conferito a decorrere dal 1° gennaio 2024 la delega al dirigente generale Capo della Direzione II in relazione alle attribuzioni in materia di debito pubblico, di cui al menzionato art. 3 del decreto del Presidente della Repubblica n. 398/2003, al fine di assicurare la continuità e la tempestività dell'azione amministrativa;

Visti i propri decreti in data 30 luglio e 28 agosto 2024, con i quali è stata disposta l'emissione delle prime quattro *tranche* dei buoni del Tesoro poliennali 3,85% con godimento 1° agosto 2024 e scadenza 1° febbraio 2035;

Ritenuto opportuno, in relazione alle condizioni di mercato, disporre l'emissione di una quinta *tranche* dei predetti buoni del Tesoro poliennali;

Decreta:

Art. 1.

Ai sensi e per gli effetti dell'art. 3 del «Testo unico» nonché del «decreto cornice», è disposta l'emissione di una quinta *tranche* dei buoni del Tesoro poliennali 3,85%, avente godimento 1° agosto 2024 e scadenza 1° febbraio 2035. L'emissione della predetta *tranche* viene disposta per un ammontare nominale compreso fra un importo minimo di 3.000 milioni di euro e un importo massimo di 3.500 milioni di euro.

I buoni fruttano l'interesse annuo lordo del 3,85%, pagabile in due semestralità posticipate, il 1° febbraio ed il 1° agosto di ogni anno di durata del prestito. La prima semestralità è pagabile il 1° febbraio 2025 e l'ultima il 1° febbraio 2035.

Sui buoni medesimi possono essere effettuate operazioni di separazione e ricostituzione delle componenti cedolari dal valore di rimborso del titolo *(«coupon stripping»)*.

Le caratteristiche e le modalità di emissione dei predetti titoli sono quelle definite nel «decreto di massima», che qui si intende interamente richiamato ed a cui si rinvia per quanto non espressamente disposto dal presente decreto.

Art. 2.

Le offerte degli operatori relative alla *tranche* di cui all'art. 1 del presente decreto dovranno pervenire entro le ore 11,00 del giorno 27 settembre 2024, con l'osservanza delle modalità indicate negli articoli 7, 8, 9, 10 e 11 del «decreto di massima».

La provvigione di collocamento, pari a 0,200% del capitale nominale sottoscritto, verrà corrisposta secondo le modalità di cui all'art. 8 del «decreto di massima» indicato nelle premesse.

Art. 3.

Al termine delle operazioni di assegnazione di cui al precedente articolo ha luogo il collocamento della sesta *tranche* dei titoli stessi, secondo le modalità indicate negli articoli 12, 13, 14 e 15 del «decreto di massima».

L'importo della *tranche* relativa al titolo oggetto della presente emissione sarà pari al 20 per cento secondo quanto stabilito dall'art. 14, comma 2, del «decreto di massima».

Gli specialisti in titoli di Stato hanno la facoltà di partecipare al collocamento supplementare, inoltrando le domande di sottoscrizione entro le ore 15,30 del giorno 30 settembre 2024.

Art. 4.

Il regolamento dei buoni sottoscritti in asta e nel collocamento supplementare sarà effettuato dagli operatori assegnatari il 1° ottobre 2024, al prezzo di aggiudicazione e con corresponsione di dietimi di interesse lordi per sessantuno giorni. A tal fine la Banca d'Italia provvederà ad inserire, in via automatica, le relative partite nel servizio di compensazione e liquidazione con valuta pari al giorno di regolamento.

In caso di ritardo nel regolamento dei titoli di cui al presente decreto, troveranno applicazione le disposizioni del regolamento (UE) n. 909/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 e del decreto ministeriale n. 12953 del 17 febbraio 2023, citati nelle premesse.

Art. 5.

Il 1° ottobre 2024 la Banca d'Italia provvederà a versare, presso la Sezione di Roma della Tesoreria dello Stato, il ricavo dei buoni assegnati al prezzo di aggiudicazione d'asta unitamente al rateo di interesse del 3,85% annuo lordo, dovuto allo Stato.

La predetta sezione di Tesoreria rilascia, per detti versamenti, separate quietanze di entrata al bilancio dello Stato, con imputazione al Capo X, capitolo 5100, art. 3 (unità di voto parlamentare 4.1.171) per l'importo relativo al ricavo dell'emissione ed al capitolo 3240, art. 3 (unità di voto parlamentare 2.1.93) per quello relativo ai dietimi d'interesse lordi dovuti.

Art. 6.

Gli oneri per interessi relativi agli anni finanziari dal 2025 al 2035, nonché l'onere per il rimborso del capitale relativo all'anno finanziario 2035, faranno carico ai capitoli che verranno iscritti nello stato di previsione della spesa del Ministero dell'economia e delle finanze per gli anni stessi e corrispondenti, rispettivamente, ai capitoli 2214 (unità di voto parlamentare 21.1) e 9502 (unità di voto parlamentare 21.2) dello stato di previsione per l'anno in corso.

L'ammontare della provvigione di collocamento, prevista dall'art. 2 del presente decreto, sarà scritturato, ad ogni cadenza di pagamento trimestrale, dalle sezioni di Tesoreria fra i «pagamenti da regolare» e farà carico al capitolo 2247 (unità di voto parlamentare 21.1; codice gestionale 109) dello stato di previsione della spesa del Ministero dell'economia e delle finanze per l'anno finanziario 2024 o a quello corrispondente per gli anni successivi.

Il presente decreto sarà pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 27 settembre 2024

p. Il direttore generale del Tesoro: IACOVONI

24A05139

DECRETI E DELIBERE DI ALTRE AUTORITÀ

COMITATO INTERMINISTERIALE PER LA PROGRAMMAZIONE ECONOMICA E LO SVILUPPO SOSTENIBILE

DELIBERA 9 luglio 2024.

Nuclei di valutazione e verifica degli investimenti pubblici. Ripartizione risorse anno 2024 (articolo 1, comma 7, della legge n. 144/1999). (Delibera n. 50/2024).

IL COMITATO INTERMINISTERIALE PER LA PROGRAMMAZIONE ECONOMICA E LO SVILUPPO SOSTENIBILE

NELLA SEDUTA DEL 9 LUGLIO 2024

Vista la legge 27 febbraio 1967, n. 48, recante «Attribuzioni e ordinamento del Ministero del bilancio e della programmazione economica e istituzione del Comitato dei Ministri per la programmazione economica» e, in particolare, l'art. 16, concernente la costituzione e le attribuzioni del Comitato interministeriale per la programmazione economica, di seguito CIPE, nonché le successive disposizioni legislative relative al Comitato, ed in particolare il decreto-legge 14 ottobre 2019, n. 111, recante «Misure urgenti per il rispetto degli obblighi previsti dalla direttiva 2008/50/CE sulla qualità dell'aria e proroga del termine di cui all'art. 48, commi 11 e 13, del decreto-legge 17 ottobre 2016, n. 189, convertito, con modificazioni, dalla legge 15 dicembre 2016, n. 229», il quale all'art. 1-*bis*, inserito nella legge di conversione 12 dicembre 2019, n. 141, ha previsto che dal 1° gennaio 2021, per «rafforzare il coordinamento delle politiche pubbliche in vista del perseguimento degli obiettivi in materia di sviluppo sostenibile indicati» dall'Agenda ONU 2030, il CIPE assuma «la denominazione di Comitato interministeriale per la programmazione economica e lo sviluppo sostenibile», di seguito CIPESS, e che «a decorrere dalla medesima data, nella legge 27 febbraio 1967, n. 48, e in ogni altra disposizione vigente, qualunque richiamo» al CIPE «deve intendersi riferito al» CIPESS;

Vista la legge 23 agosto 1988, n. 400, recante «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei ministri», e successive modificazioni, e in particolare, l'art. 5, comma 2;

Visto il decreto del Presidente del Consiglio dei ministri 1° ottobre 2012, e successive modificazioni, recante

«Ordinamento delle strutture generali della Presidenza del Consiglio dei ministri», e, in particolare, l'art. 20, relativo all'organizzazione e ai compiti del Dipartimento per la programmazione e il coordinamento della politica economica, di seguito DIPE;

Vista la legge 17 maggio 1999, n. 144 recante «Misure in materia di investimenti, delega al Governo per il riordino degli incentivi all'occupazione e della normativa che disciplina l'INAIL, nonché disposizioni per il riordino degli enti previdenziali», e successive modificazioni, in particolare, l'art. 1, comma 7, che prevede l'istituzione di un Fondo da ripartire, di seguito Fondo, previa deliberazione di questo Comitato, sentita la Conferenza permanente per i rapporti tra lo Stato, le regioni e le Province autonome di Trento e Bolzano, di seguito CSR, finalizzato al cofinanziamento delle attività dei Nuclei di valutazione e verifica degli investimenti pubblici, presso le amministrazioni centrali e regionali, di seguito Nuclei, ivi comprese le funzioni orizzontali, rappresentate dal ruolo di coordinamento in capo a questo Comitato e dal sistema di monitoraggio degli investimenti pubblici, di seguito MIP, istituito presso questo stesso Comitato;

Visto l'art. 145, comma 10, della legge 23 dicembre 2000, n. 388 recante «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» (Legge finanziaria 2001), in base al quale le risorse stanziate per il citato Fondo potranno cofinanziare, tra l'altro, l'avvio del Sistema MIP e le spese relative al funzionamento della rete dei Nuclei e al ruolo di coordinamento svolto da questo Comitato;

Visto l'art. 11 della legge 16 gennaio 2003, n. 3 recante «Disposizioni ordinamentali in materia di pubblica amministrazione», e successive modificazioni, il quale stabilisce che, per le finalità del MIP, ogni nuovo progetto di investimento pubblico sia dotato di un Codice unico di progetto, di seguito CUP;

Visto l'art. 2, comma 109, della legge 23 dicembre 2009, n. 191 recante «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» (Legge finanziaria 2010), in seguito al quale risultano esclusi dal riparto i Nuclei delle Province autonome di Trento e Bolzano, a titolo di concorso delle medesime province al riequilibrio di finanza pubblica secondo quanto previsto dall'art. 79 del decreto del Presidente della Repubblica 31 agosto 1972, n. 670 (Statuto speciale per il Trentino Alto Adige);

Vista la legge 13 agosto 2010, n. 136, recante «Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia» e successive modificazioni, ed in particolare gli articoli 3 e 6 concernenti rispettivamente l'utilizzo del CUP per assicurare la tracciabilità dei flussi finanziari finalizzata a prevenire infiltrazioni criminali, e la sanzione per il suo mancato utilizzo;

Visto il decreto legislativo 29 dicembre 2011, n. 228, recante «Attuazione dell'art. 30, comma 9, lettere *a)*, *b)*, *c)* e *d)*, della legge 31 dicembre 2009, n. 196, in materia di valutazione degli investimenti relativi ad opere pubbliche», e in particolare l'art. 7, comma 1 il quale prevede che i Ministeri individuino nei Nuclei gli organismi responsabili delle attività di valutazione;

Visto il decreto legislativo 29 dicembre 2011, n. 229, recante «Attuazione dell'art. 30, comma 9, lettere *e)*, *f)* e *g)* della legge 31 dicembre 2009, n. 196, in materia di monitoraggio sullo stato di attuazione delle opere pubbliche, di verifica dell'utilizzo dei finanziamenti nei tempi previsti e costituzione del Fondo opere e del Fondo progetti», ed in particolare l'art. 1, comma 1, lettera *d)*, il quale prescrive che nell'ambito dei sistemi informativi indicati nel citato articolo: «l'opera sia corredata, ai fini dell'ottenimento dei relativi finanziamenti pubblici, del Codice unico di progetto (CUP) che deve figurare già nella fase di presentazione ed in tutte le successive transazioni, anche ai sensi della legge 13 agosto 2010, n. 136. Il Codice identificativo di gara non può essere rilasciato dall'autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture nei confronti di contratti finalizzati alla realizzazione di progetti d'investimento pubblico sprovvisti del Codice unico di progetto obbligatorio ai sensi dell'art. 11 della legge 16 gennaio 2003, n. 3, e successive modificazioni.»

Visto il decreto del Presidente del Consiglio dei ministri 21 dicembre 2012, n. 262, previsto dall'art. 7, comma 3, del citato decreto legislativo n. 228 del 2011, recante «Disciplina dei nuclei istituiti presso amministrazioni centrali dello Stato con la funzione di garantire supporto tecnico alla programmazione, valutazione e monitoraggio degli interventi pubblici»;

Visto l'art. 41, comma 2, del decreto-legge 16 luglio 2020, n. 76, recante «Misure urgenti per la semplificazione e l'innovazione digitale», convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120, che ha modificato l'art. 1, comma 7, della citata legge 17 maggio 1999, n. 144, disponendo, dall'anno 2021, l'assegnazione annuale di 900.000 euro per il funzionamento del Sistema MIP/CUP;

Visto l'art. 50, comma 10, del decreto-legge 24 febbraio 2023, n. 13, recante «Disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e del Piano nazionale degli investimenti complementari al PNRR (PNC), nonchè per l'attuazione delle politiche di coesione e della politica agricola comune» convertito, con modificazioni, dalla legge 21 aprile 2023, n. 41, il quale prevede la: "riorganizzazione, senza nuovi o maggiori oneri a carico della finanza pubblica, del Nucleo di valutazione e analisi per la programmazione (NUVAP) di cui all'art. 1, comma 2, del decreto del Presidente del Consiglio dei ministri 19 novembre 2014, pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana - n. 300 del 29 dicembre 2014, che viene ridenominato

“Nucleo per le politiche di coesione (NUPC)” e al quale sono trasferite le funzioni e le attività attribuite dalle vigenti disposizioni al Nucleo di verifica e controllo di cui all’art. 1, comma 3, del decreto del Presidente del Consiglio dei ministri 19 novembre 2014, pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana - n. 300 del 29 dicembre 2014”»;

Visto il decreto del Presidente del Consiglio dei ministri del 13 dicembre 2023, di approvazione del bilancio di previsione della Presidenza del Consiglio dei ministri per l’anno 2024, con il quale sono stati assegnati al Fondo euro 2.811.210,00;

Ritenuto che anche per il 2024 le attività di raccordo poste in capo al Dipartimento per la programmazione e il coordinamento della politica economica della Presidenza del Consiglio dei ministri, di seguito DIPE, siano svolte senza aggravio per il citato Fondo;

Vista la delibera CIPE 18 marzo 2013, n. 26, ed in particolare il punto 6, in cui si dispone che «I Nuclei invieranno una relazione annuale, da predisporre entro il 31 gennaio di ogni anno, sulle attività svolte e sulla spesa sostenuta a valere sia sulle assegnazioni CIPE sia sul cofinanziamento da parte delle amministrazioni di appartenenza»;

Vista la delibera CIPE 22 dicembre 2017, n. 126, con la quale è stato previsto che il DIPE istituisse un Tavolo permanente per assicurare la governance multilivello ed il presidio costante delle disponibilità del Fondo e della continuità e adeguatezza dei flussi finanziari;

Vista la nota 10 luglio 2017, n. 3396, con la quale il DIPE ha trasmesso la proposta di revisione dei criteri di riparto delle risorse destinate al cofinanziamento delle spese di funzionamento dei Nuclei alla CSR, ai fini dell’espressione del parere di competenza;

Considerato che la CSR, con parere 27 luglio 2017, n. 114, ha approvato la sopracitata proposta;

Considerato che il DIPE ha convocato periodicamente il sopracitato Tavolo permanente la cui ultima riunione annuale si è tenuta in data 16 aprile 2024;

Vista la nota prot. DIPE n. 5164 del 22 maggio 2024, con la quale il DIPE ha trasmesso alla CSR la proposta di riparto del Fondo destinato al co-finanziamento delle spese di funzionamento dei nuclei di valutazione e verifica degli investimenti pubblici delle amministrazioni centrali e regionali per l’annualità 2024;

Considerato che nella seduta del 14 giugno 2024 la CSR si è espressa favorevolmente con parere n. 91/CSR in merito alla suddetta proposta di riparto del Fondo destinato al co-finanziamento delle spese di funzionamento dei nuclei di valutazione e verifica degli investimenti pubblici delle amministrazioni centrali e regionali per l’annualità 2024;

Visto il decreto del Presidente della Repubblica del 31 ottobre 2022, con il quale il senatore Alessandro Morelli è stato nominato Sottosegretario di Stato alla Presidenza del Consiglio dei ministri;

Visto il decreto del Presidente del Consiglio dei ministri 25 novembre 2022, con il quale il senatore Alessandro Morelli è stato nominato segretario del Comitato interministeriale per la programmazione economica e lo sviluppo sostenibile (CIPESS), e gli è stata assegnata, tra le altre, la delega ad esercitare le funzioni spettanti al Presidente del Consiglio dei ministri in materia di coordinamento della politica economica e di programmazione e monitoraggio degli investimenti pubblici, compresi quelli orientati al perseguimento dello sviluppo sostenibile, nonché quelli in regime di partenariato pubblico-privato;

Vista la nota dell’ufficio del sottosegretario USS 19 giugno 2024, n. 327 acquista con Prot. DIPE n. 6358 del 20 giugno 2024, con la quale il segretario del CIPESS propone l’inserimento all’ordine del giorno di questo Comitato della proposta di riparto del Fondo destinato al co-finanziamento delle spese di funzionamento dei nuclei di valutazione e verifica degli investimenti pubblici delle amministrazioni centrali e regionali per l’annualità 2024;

Tenuto conto dell’esame della proposta oggetto della presente delibera svolto ai sensi del regolamento interno di questo Comitato, approvato con delibera 28 novembre 2018, n. 82, recante «Regolamento interno del Comitato interministeriale per la programmazione economica» come modificata dalla delibera 15 dicembre 2020, n. 79, recante «Regolamento interno del Comitato interministeriale per la programmazione economica e lo sviluppo sostenibile (CIPESS)»;

Vista la nota 9 luglio 2024, n. 7106, predisposta congiuntamente dal DIPE e dal Ministero dell’economia e delle finanze, posta a base dell’odierna seduta del Comitato, contenente le valutazioni istruttorie in merito alla presente delibera;

Considerato il dibattito svoltosi durante la seduta odierna del Comitato;

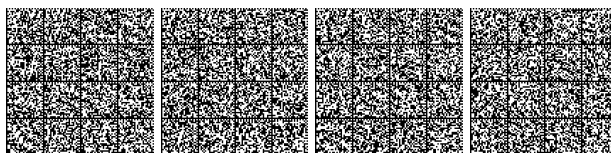
Su proposta del segretario di questo Comitato;

Delibera:

1. È approvato il riparto per l’anno 2024 del Fondo di cui all’art. 1, comma 7, della legge 17 maggio 1999, n. 144, secondo lo schema di cui alla tabella 1 seguente:

Tabella 1 - Proposta di riparto del Fondo - Anno 2024

(legge n. 144/1999, art. 1, comma 7)

Sezione 1 - Regioni	
Abruzzo	66.783,39
Basilicata	75.759,61
Calabria	87.515,34
Campania	139.875,84
Emilia-Romagna	93.784,27
Friuli V-Giulia	62.980,65
Lazio	106.635,23
Liguria	69.570,58
Lombardia	108.879,21
Marche	46.040,28
Molise	39.157,40
Piemonte	92.685,66
Puglia	112.536,33
Sardegna	81.969,75
Sicilia	135.144,89
Toscana	85.674,08
Umbria	58.863,36
Valle d'Aosta	53.774,46
Veneto	100.630,93
Totale	**1.618.261,27**

Sezione 2 - Amministrazioni centrali	
Politiche agricole	36.618,59
Giustizia	36.618,59
Cultura	36.618,59
MIT	36.618,59
Salute	36.618,59
Interno	36.618,59
PCM-DIPE	36.618,59
Totale	**256.330,14**
Sezione 3 - Funzioni orizzontali	
MIP/CUP	900.000,00
PCM-NUPC (ex NUVAP)	36.618,59
Totale	**936.618,59**
Totale Fondo anno 2024	**2.811.210,00**

Il vice Presidente: GIORGETTI

Il Segretario: MORELLI

Registrato alla Corte dei conti il 17 settembre 2024
Ufficio di controllo sugli atti del Ministero dell'economia e delle finanze, n. 1249

24A05073

ESTRATTI, SUNTI E COMUNICATI

AGENZIA ITALIANA DEL FARMACO

Autorizzazione all'immissione in commercio del medicinale per uso umano, a base di dorzolamide cloridrato e timololo maleato, «Dorzolamide Timololo Omnivision».

Estratto determina AAM/A.I.C. n. 204 del 12 settembre 2024

Procedura europea n. AT/H/1213/001/DC.

È autorizzata l'immissione in commercio del medicinale DORZOLAMIDE/TIMOLOLO OMNIVISION, le cui caratteristiche sono riepilogate nel riassunto delle caratteristiche del prodotto (RCP), foglio illustrativo (FI) ed etichette (Eti), parti integranti della determina di cui al presente estratto, nelle forme farmaceutiche, dosaggio e confezione alle condizioni e con le specificazioni di seguito indicate.

Titolare A.I.C.: OmniVision Italia S.r.l., con sede legale e domicilio fiscale in - via Montefeltro n. 6 - 20156 Milano, Italia.

Confezioni:

«20 mg/mL+ 5 mg/mL collirio, soluzione» 1 contenitore HDPE da 5 mL con pompa contagocce - A.I.C. n. 051124016 (in base 10) 1JS5TJ (in base 32);

«20 mg/mL + 5 mg/mL collirio, soluzione» 1 contenitore HDPE da 9 mL con pompa contagocce - A.I.C. n. 051124028 (in base 10) 1JS5TW (in base 32);

«20 mg/mL + 5 mg/mL collirio, soluzione» 2 contenitori HDPE da 9 mL con pompa contagocce - A.I.C. n. 051124030 (in base 10) 1JS5TY (in base 32).

Principi attivi: dorzolamide cloridrato e timololo maleato.

Produttore responsabile del rilascio dei lotti:

Tubilux Pharma S.p.a. - via Costarica n. 20/22 - 00071, Pomezia (Roma).

Classificazione ai fini della rimborsabilità

Per le confezioni sopra riportate è adottata la seguente classificazione ai fini della rimborsabilità:

classificazione ai fini della rimborsabilità: apposita sezione della classe di cui all'art. 8, comma 10, lettera *c)* della legge 24 dicembre 1993, n. 537 e successive modificazioni, dedicata ai farmaci non ancora valutati ai fini della rimborsabilità, denominata classe C(nn).

Classificazione ai fini della fornitura

Per le confezioni sopra riportate è adottata la seguente classificazione ai fini della fornitura:

classificazione ai fini della fornitura: RR: medicinale soggetto a prescrizione medica.

Stampati

Le confezioni del medicinale devono essere poste in commercio con etichette e fogli illustrativi conformi al testo allegato alla determina, di cui al presente estratto.

È approvato il riassunto delle caratteristiche del prodotto allegato alla determina, di cui al presente estratto.

In ottemperanza all'art. 80, commi 1 e 3 del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni il foglio illustrativo e le etichette devono essere redatti in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Tutela di mercato

Il titolare dell'A.I.C. del farmaco generico è esclusivo responsabile del pieno rispetto dei termini previsti dall'art. 10, commi 2 e 4, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, secondo cui un medicinale generico non può essere immesso in commercio, finché non siano trascorsi dieci anni dall'autorizzazione iniziale del medicinale di riferimento, ovvero, finché non siano trascorsi undici anni dall'autorizzazione iniziale del medicinale di riferimento, se durante i primi otto anni di tale decennio, il titolare dell'A.I.C. abbia ottenuto un'autorizzazione per una o più indicazioni terapeutiche nuove che, dalla valutazione scientifica preliminare all'autorizzazione, sono state ritenute tali da apportare un beneficio clinico rilevante rispetto alle terapie esistenti.

Il presente paragrafo e la contenuta prescrizione sono da ritenersi applicabili solo ove si realizzi la descritta fattispecie.

Tutela brevettuale

Il titolare dell'A.I.C. del farmaco generico è esclusivo responsabile del pieno rispetto dei diritti di proprietà industriale relativi al medicinale di riferimento e delle vigenti disposizioni normative in materia brevettuale.

Il titolare dell'A.I.C. è altresì responsabile del pieno rispetto di quanto disposto dall'art. 14, comma 2 del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, in virtù del quale non sono incluse negli stampati quelle parti del riassunto delle caratteristiche del prodotto del medicinale di riferimento che si riferiscono a indicazioni o a dosaggi ancora coperti da brevetto al momento dell'immissione in commercio del medicinale.

Il presente paragrafo e la contenuta prescrizione sono da ritenersi applicabili solo ove si realizzi la descritta fattispecie.

Rapporti periodici di aggiornamento sulla sicurezza – PSUR

Il titolare dell'autorizzazione all'immissione in commercio deve fornire i rapporti periodici di aggiornamento sulla sicurezza per questo medicinale conformemente ai requisiti definiti nell'elenco delle date di riferimento per l'Unione europea (elenco EURD) di cui all'art. 107-*quater*, par. 7) della direttiva 2010/84/CE e pubblicato sul portale web dell'Agenzia europea dei medicinali.

Condizioni o limitazioni per quanto riguarda l'uso sicuro ed efficace del medicinale

Il titolare dell'autorizzazione all'immissione in commercio è tenuto a porre in essere le attività e le azioni di farmacovigilanza richieste e dettagliate nel Piano di gestione del rischio (RMP).

Validità dell'autorizzazione

L'autorizzazione ha validità fino alla data comune di rinnovo europeo (CRD) 15 marzo 2029, come indicata nella notifica di fine procedura (EoP) trasmessa dallo Stato membro di riferimento (RMS).

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05011

Autorizzazione all'immissione in commercio del medicinale per uso umano, a base di ciclopentolato cloridrato, «Plegik».

Estratto determina AAM/A.I.C. n. 214/2024 del 18 settembre 2024

È autorizzata l'immissione in commercio del medicinale PLEGIK le cui caratteristiche sono riepilogate nel riassunto delle caratteristiche del prodotto (RCP), foglio illustrativo (FI) ed etichette (Eti), parti integranti della determina di cui al presente estratto, nella forma farmaceutica, dosaggio e confezione alle condizioni e con le specificazioni di seguito indicate.

Titolare A.I.C.: Medivis S.r.l., con sede e domicilio fiscale in via Carnazza, 34/C - 95030 Tremestieri Etneo - Catania, Italia.

Confezione: «10 mg/ml collirio, soluzione» 1 flacone in LDPE da 5 ml con contagocce.

A.I.C. n. 049916012 (in base 10) 1HMB3D (in base 32).

Principio attivo: ciclopentolato cloridrato.

Produttori responsabili del rilascio dei lotti:

Laboratorio Edol - Produtos Farmacèuticos, S.A., Av. 25 de Abril, 6-6a, 2795-225 Linda-a-Velha, Portogallo;

Laboratorio Edol - Produtos Farmacèuticos, S.A., Rua Quinta Do Salrego N 22-22a, Portela De Carnaxide, Carnaxide, 2790-144 - Rua Casal Do Canas 6-6a, Carnaxide, 2790-204, Portogallo.

Classificazione ai fini della rimborsabilità

Confezione A.I.C. n. 049916012 «10 mg/ml collirio, soluzione» 1 flacone in LDPE da 5 ml con contagocce.

Classificazione ai fini della rimborsabilità: apposita sezione della classe di cui all'art. 8, comma 10, lettera *c)*, della legge 24 dicembre 1993, n. 537 e successive modificazioni, dedicata ai farmaci non ancora valutati ai fini della rimborsabilità, denominata classe C(nn).

Classificazione ai fini della fornitura

Confezione: A.I.C. n. 049916012 «10 mg/ml collirio, soluzione» 1 flacone in LDPE da 5 ml con contagocce.

Classificazione ai fini della fornitura: RR - medicinale soggetto a prescrizione medica.

Stampati

Le confezioni del medicinale devono essere poste in commercio con etichette e fogli illustrativi conformi al testo allegato alla determina, di cui al presente estratto.

È approvato il riassunto delle caratteristiche del prodotto allegato alla determina, di cui al presente estratto.

In ottemperanza all'art. 80, commi 1 e 3, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, il foglio illustrativo e le etichette devono essere redatti in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Tutela di mercato

Il titolare dell'A.I.C. del farmaco generico è esclusivo responsabile del pieno rispetto dei termini previsti dall'art. 10, commi 2 e 4, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, secondo cui un medicinale generico non può essere immesso in commercio, finché non siano trascorsi dieci anni dall'autorizzazione iniziale del medicinale di riferimento, ovvero, finché non siano trascorsi undici anni dall'autorizzazione iniziale del medicinale di riferimento,

se durante i primi otto anni di tale decennio, il titolare dell'A.I.C. abbia ottenuto un'autorizzazione per una o più indicazioni terapeutiche nuove che, dalla valutazione scientifica preliminare all'autorizzazione, sono state ritenute tali da apportare un beneficio clinico rilevante rispetto alle terapie esistenti.

Il presente paragrafo e la contenuta prescrizione sono da ritenersi applicabili solo ove si realizzi la descritta fattispecie.

Tutela brevettuale

Il titolare dell'A.I.C. del farmaco generico è esclusivo responsabile del pieno rispetto dei diritti di proprietà industriale relativi al medicinale di riferimento e delle vigenti disposizioni normative in materia brevettuale.

Il titolare dell'A.I.C. è altresì responsabile del pieno rispetto di quanto disposto dall'art. 14, comma 2, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, in virtù del quale non sono incluse negli stampati quelle parti del riassunto delle caratteristiche del prodotto del medicinale di riferimento che si riferiscono a indicazioni o a dosaggi ancora coperti da brevetto al momento dell'immissione in commercio del medicinale.

Il presente paragrafo e la contenuta prescrizione sono da ritenersi applicabili solo ove si realizzi la descritta fattispecie.

Rapporti periodici di aggiornamento sulla sicurezza - PSUR

Il titolare dell'autorizzazione all'immissione in commercio deve fornire i rapporti periodici di aggiornamento sulla sicurezza per questo medicinale conformemente ai requisiti definiti nell'elenco delle date di riferimento per l'Unione europea (elenco EURD) di cui all'art. 107-*quater*, par. 7), della direttiva 2010/84/CE e pubblicato sul portale *web* dell'Agenzia europea dei medicinali.

Condizioni o limitazioni per quanto riguarda l'uso sicuro ed efficace del medicinale

Il titolare dell'autorizzazione all'immissione in commercio è tenuto a porre in essere le attività e le azioni di farmacovigilanza richieste e dettagliate nel Piano di gestione del rischio (RMP).

Validità dell'autorizzazione

L'autorizzazione ha validità di cinque anni a decorrere dalla data di efficacia della presente determina.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05012

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di clotrimazolo, «Clozol».

Estratto determina AAM/PPA n. 714/2024 del 13 settembre 2024

Trasferimento di titolarità: AIN/2024/1395.

È autorizzato il trasferimento di titolarità dell'autorizzazione all'immissione in commercio del sotto elencato medicinale fino ad ora registrato a nome della società FG S.r.l. con sede legale e domicilio fiscale in via San Rocco, 6, 85033 Episcopia, Potenza, codice fiscale 01444240764.

Medicinale: CLOZOL.

Confezione: «2% crema vaginale» 1 tubo in al da 30 g con 6 applicatori monouso.

A.I.C. n. 049989015,

alla società Farmitalia Industria chimico farmaceutica S.r.l. con sede legale e domicilio fiscale in via Pinciana, 25, 00198 Roma, codice fiscale 03115090874.

Stampati

Il titolare dell'autorizzazione all'immissione in commercio del medicinale sopraindicato deve apportare le necessarie modifiche al riassunto delle caratteristiche del prodotto dalla data di entrata in vigore della determina, di cui al presente estratto; al foglio illustrativo ed alle etichette dal primo lotto di produzione successivo all'entrata in vigore della determina, di cui al presente estratto.

Smaltimento scorte

I lotti del medicinale, già prodotti e rilasciati a nome del precedente titolare alla data di entrata in vigore della determina, di cui al presente estratto, possono essere mantenuti in commercio fino alla data di scadenza indicata in etichetta.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05014

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di meropenem, «Merrem».

Estratto determina AAM/PPA n. 717/2024 del 13 giugno 2024

L'autorizzazione all'immissione in commercio è modificata, a seguito della variazione approvata dallo Stato membro di riferimento (Francia):

Tipo II - C.I.4) Modifica dei paragrafi 4.4, 4.8 e 5.1 del riassunto delle caratteristiche del prodotto e paragrafo 4 del foglio illustrativo,

relativamente al medicinale MERREM nella forma farmaceutica, dosaggio e confezioni di seguito indicate:

confezione «500 mg polvere per soluzione iniettabile per uso endovenoso» 10 flaconcini - A.I.C. n. 028949081;

confezione «1000 mg polvere per soluzione iniettabile per uso endovenoso» 10 flaconcini - A.I.C. n. 028949093.

Codice pratica: VC2/2023/520.

Numero procedura: FR/H/0467/001-002/II/042.

Titolare: Pfizer Italia S.r.l., con sede legale e domicilio fiscale in via Isonzo n. 71 - 04100 Latina, codice fiscale 06954380157.

Gli stampati corretti e approvati sono allegati alla determina, di cui al presente estratto.

Stampati

1. Il titolare dell'autorizzazione all'immissione in commercio deve apportare le modifiche autorizzate, dalla data di entrata in vigore della determina, di cui al presente estratto, al riassunto delle caratteristiche del prodotto; entro e non oltre i sei mesi dalla medesima data al foglio illustrativo.

2. In ottemperanza all'art. 80, commi 1 e 3, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, il foglio illustrativo e le etichette devono essere redatti in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Smaltimento scorte

Sia i lotti già prodotti alla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto che i lotti prodotti nel periodo di cui al precedente paragrafo del presente estratto, che non riportino le modifiche autorizzate, possono essere mantenuti in commercio fino alla data di scadenza del medicinale indicata in etichetta. A decorrere dal termine di trenta giorni dalla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto, i farmacisti sono tenuti a consegnare il foglio illustrativo aggiornato agli utenti, che scelgono la modalità di ritiro in formato cartaceo o analogico o mediante l'utilizzo di metodi digitali alternativi. Il titolare A.I.C. rende accessibile al farmacista il foglio illustrativo aggiornato entro il medesimo termine.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05015

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di destrometorfano bromidrato, «Vicks Tosse Sedativo».

Estratto determina AAM/PPA n. 713/2024 del 13 settembre 2024

È autorizzata la seguente variazione:

tipo II - C.I.4). È modificato il paragrafo 5.1 del riassunto delle caratteristiche del prodotto relativamente al medicinale VICKS TOSSE SEDATIVO nella forma farmaceutica, dosaggio e confezioni di seguito elencate:

A.I.C. n. 028688012 - «1,33 mg/ml sciroppo» flacone 120 ml;

A.I.C. n. 028688024 - «1,33 mg/ml sciroppo» flacone 180 ml.

È approvata, altresì, secondo la lista dei termini standard della Farmacopea europea, la modifica della denominazione delle confezioni già autorizzate come di seguito indicato:

da: A.I.C. n. 028688012 - «1,33 mg/ml sciroppo» flacone 120 ml;

a: A.I.C. n. 028688012 - «1,33 mg/ml sciroppo» 1 flacone in vetro da 120 ml con chiusura a prova di bambino;

da: A.I.C. n. 028688024 - «1,33 mg/ml sciroppo» flacone 180 ml;

a: A.I.C. n. 028688024 - «1,33 mg/ml sciroppo» 1 flacone in vetro da 180 ml con chiusura a prova di bambino.

Codice pratica: VN2/2024/94.

Titolare A.I.C.: Procter & Gamble S.r.l., con sede legale e domicilio fiscale in viale Giorgio Ribotta, 11 - 00144 Roma, codice fiscale 05858891004.

Gli stampati corretti e approvati sono allegati alla determina, di cui al presente estratto.

Stampati

1. Il titolare dell'autorizzazione all'immissione in commercio deve apportare le modifiche autorizzate, dalla data di entrata in vigore della determina, di cui al presente estratto, al riassunto delle caratteristiche del prodotto.

2. In ottemperanza all'art. 80, commi 1 e 3, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, il foglio illustrativo e le etichette devono essere redatti in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Smaltimento scorte

Sia i lotti già prodotti alla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto, che i lotti prodotti nel periodo di cui al precedente paragrafo del presente estratto, possono essere mantenuti in commercio fino alla data di scadenza del medicinale indicata in etichetta, ai sensi dell'art. 1, comma 7, della determina AIFA n. DG/821/2018 del 24 maggio 2018, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana n. 133 dell'11 giugno 2018.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05016

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di estratto secco di cimicifuga recamosa (L.) Nutt., rhizoma, «Cimifemin».

Estratto determina AAM/PPA n. 746/2024 del 20 settembre 2024

Trasferimento di titolarità: AIN/2024/1352.

È autorizzato il trasferimento di titolarità dell'autorizzazione all'immissione in commercio del sotto elencato medicinale fino ad ora registrato a nome della società Yes Pharmaceutical Development Services GmbH, con sede legale in Basler Strasse, 7 - 61352 - Bad Homburg, Germania.

Medicinale: CIMIFEMIN.

Confezioni:

049810017 - «2,5 mg compresse» 20 compresse in blister PVC/PVDC/AL;

049810029 - «2,5 mg compresse» 60 compresse in blister PVC/PVDC/AL;

049810031- «2,5 mg compresse» 100 compresse in blister PVC/PVDC/AL,

alla società Schaper & Brummer GmbH & Co. Kg, con sede legale in Bahnhofstrasse, 35, 38259 - Salzgitter, Germania.

Stampati

Il titolare dell'autorizzazione all'immissione in commercio del medicinale sopraindicato deve apportare le necessarie modifiche al riassunto delle caratteristiche del prodotto dalla data di entrata in vigore della determina, di cui al presente estratto; al foglio illustrativo ed alle etichette dal primo lotto di produzione successivo all'entrata in vigore della determina, di cui al presente estratto.

Smaltimento scorte

I lotti del medicinale, già prodotti e rilasciati a nome del precedente titolare alla data di entrata in vigore della determina, di cui al presente estratto, possono essere mantenuti in commercio fino alla data di scadenza indicata in etichetta.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05033

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di [18F] PSMA-1007, «Radelumin».

Estratto determina AAM/PPA n. 739/2024 del 20 settembre 2024

L'autorizzazione all'immissione in commercio è modificata, a seguito delle seguenti variazioni, approvate dallo Stato membro di riferimento (RMS), con procedura FR/H/0797/II/005/G, relativamente al medicinale RADELUMIN:

Tipo IA_{IN}, B.II.b.2 - modifiche a livello di importatore, di modalità di rilascio dei lotti e di prove di controllo qualitativo del prodotto finito; *c)* sostituzione o aggiunta di un fabbricante responsabile dell'importazione e/o del rilascio dei lotti; 2. compresi il controllo dei lotti/le prove:

Synektik Pharma Sp z o.o., Szaserów Street 128, 04-141, Warszawa, Poland, quale responsabile del rilascio lotti del prodotto finito;

Tipo IA_{IN}, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *a)* sito di confezionamento secondario;

Tipo II, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *c)* sito in cui sono effettuate tutte le operazioni di fabbricazione, ad eccezione del rilascio dei lotti, del controllo dei lotti e del confezionamento secondario, o destinato alle forme farmaceutiche prodotte attraverso procedimenti di fabbricazione complessi;

Tipo II, B.I.a.1 - modifica del fabbricante di una materia prima, di un reattivo o di un prodotto intermedio utilizzati nel procedimento di

fabbricazione di un principio attivo o modifica del fabbricante del principio attivo (compresi eventualmente i siti di controllo della qualità), per i quali non si dispone di un certificato di conformità alla farmacopea europea; *g)* introduzione di un nuovo fabbricante del principio attivo che non ha il sostegno di un ASMF e che richiede un aggiornamento significativo della pertinente sezione del fascicolo del principio attivo.

Si modificano gli stampati, paragrafo 6 del Foglio Illustrativo, come descritto:

6. Contenuto della confezione e altre informazioni

[...]

Produttori:

[...]

Synektik Pharma Sp. z o.o. ul. Szaserów 128, 04-141, Warszawa, Polonia.

L'autorizzazione all'immissione in commercio è modificata, a seguito delle seguenti variazioni, approvate dallo Stato membro di riferimento (RMS), con procedura FR/H/0797/II/011/G, relativamente al medicinale RADELUMIN:

Tipo IA, n. 2 variazioni, B.II.b.2 - modifiche a livello di importatore, di modalità di rilascio dei lotti e di prove di controllo qualitativo del prodotto finito; *a)* sostituzione o aggiunta di un sito in cui si effettuano il controllo dei lotti/le prove;

Tipo IA_{IN}, B.II.b.2 - modifiche a livello di importatore, di modalità di rilascio dei lotti e di prove di controllo qualitativo del prodotto finito; *c)* sostituzione o aggiunta di un fabbricante responsabile dell'importazione e/o del rilascio dei lotti; 2. compresi il controllo dei lotti/le prove:

Synektik Pharma Sp. z o.o., Artwińskiego Street 3, 25-734 Kielce, Polonia, quale responsabile del rilascio lotti del prodotto finito;

Tipo IA_{IN}, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *a)* sito di confezionamento secondario;

Tipo II, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *c)* sito in cui sono effettuate tutte le operazioni di fabbricazione, ad eccezione del rilascio dei lotti, del controllo dei lotti e del confezionamento secondario, o destinato alle forme farmaceutiche prodotte attraverso procedimenti di fabbricazione complessi;

Tipo II, B.I.a.1 - modifica del fabbricante di una materia prima, di un reattivo o di un prodotto intermedio utilizzati nel procedimento di fabbricazione di un principio attivo o modifica del fabbricante del principio attivo (compresi eventualmente i siti di controllo della qualità), per i quali non si dispone di un certificato di conformità alla farmacopea europea; *g)* introduzione di un nuovo fabbricante del principio attivo che non ha il sostegno di un ASMF e che richiede un aggiornamento significativo della pertinente sezione del fascicolo del principio attivo.

Si modificano gli stampati, paragrafo 6 del foglio illustrativo, come descritto:

6. Contenuto della confezione e altre informazioni

[...]

Produttori:

[...]

Synektik Pharma Sp. z o.o. ul. Artwińskiego 3, 25-734 Kielce, Polonia.

Confezioni e numeri A.I.C.:

050594011 - «1300 mbq/ml soluzione iniettabile» 1 flaconcino multidose in vetro da 10 ml contenente da 0,3 ml a 10 ml;

050594023 - «1300 mbq/ml soluzione iniettabile» 1 flaconcino multidose in vetro da 15 ml contenente da 0,3 ml a 15 ml;

050594035 - «1300 mbq/ml soluzione iniettabile» 1 flaconcino multidose in vetro da 20 ml contenente da 0,3 ml a 20 ml.

Titolare A.I.C.: ABX advanced biochemical compounds - Biomedizinische Forschungsreagenzien GmbH, con sede legale e domicilio fiscale in Heinrich-Gläser-Straße 10-14, 01454 Radeberg, Germania.

Procedure europea: FR/H/0797/II/005/G - FR/H/0797/II/011/G.

Codici pratica: VC2/2023/241 - VC2/2023/289.

Stampati

Il titolare dell'autorizzazione all'immissione in commercio deve apportare le modifiche autorizzate, dalla data di entrata in vigore della determina, di cui al presente estratto, al riassunto delle caratteristiche del prodotto; entro e non oltre i sei mesi dalla medesima data al foglio illustrativo.

In ottemperanza all'art. 80, commi 1 e 3, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, il foglio illustrativo deve essere redatto in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Smaltimento scorte

Sia i lotti già prodotti alla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto che i lotti prodotti nel periodo di cui al precedente paragrafo del presente estratto, che non riportino le modifiche autorizzate, possono essere mantenuti in commercio fino alla data di scadenza del medicinale indicata in etichetta, ai sensi dell'art. 1, comma 7 della determina AIFA n. DG/821/2018 del 24 maggio 2018, pubblicata nella *Gazzetta Ufficiale* n. 133 dell'11 giugno 2018.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05053

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di [18F] PSMA-1007, «Radelumin».

Estratto determina AAM/PPA n. 741/2024 del 20 settembre 2024

L'autorizzazione all'immissione in commercio è modificata, a seguito delle seguenti variazioni, approvate dallo Stato membro di riferimento (RMS), con procedura FR/H/0797/II/013/G, relativamente al medicinale RADELUMIN:

tipo IA_{IN}, B.II.b.2 - modifiche a livello di importatore, di modalità di rilascio dei lotti e di prove di controllo qualitativo del prodotto finito; *c)* sostituzione o aggiunta di un fabbricante responsabile dell'importazione e/o del rilascio dei lotti; 2. compresi il controllo dei lotti/le prove:

Seibersdorf Labor GmbH, 2444 Seibersdorf, Austria;

tipo IA_{IN}, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *a)* sito di confezionamento secondario;

tipo II, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *c)* sito in cui sono effettuate tutte le operazioni di fabbricazione, ad eccezione del rilascio dei lotti, del controllo dei lotti e del confezionamento secondario, o destinato alle forme farmaceutiche prodotte attraverso procedimenti di fabbricazione complessi;

tipo II, B.I.a.1 - modifica del fabbricante di una materia prima, di un reattivo o di un prodotto intermedio utilizzati nel procedimento di fabbricazione di un principio attivo o modifica del fabbricante del principio attivo (compresi eventualmente i siti di controllo della qualità), per i quali non si dispone di un certificato di conformità alla farmacopea europea; *g)* introduzione di un nuovo fabbricante del principio attivo che non ha il sostegno di un ASMF e che richiede un aggiornamento significativo della pertinente sezione del fascicolo del principio attivo;

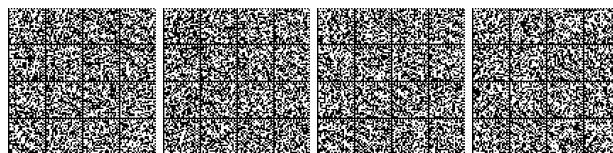
tipo IA, B.II.b.2 - modifiche a livello di importatore, di modalità di rilascio dei lotti e di prove di controllo qualitativo del prodotto finito; *a)* sostituzione o aggiunta di un sito in cui si effettuano il controllo dei lotti/le prove.

Si modificano gli stampati, paragrafo 6 del foglio illustrativo, come descritto:

6. Contenuto della confezione e altre informazioni

[…]

Produttori:

[…]

Seibersdorf Labor GmbH, 2444 Seibersdorf, Austria.

L'autorizzazione all'immissione in commercio è modificata, a seguito delle seguenti variazioni, approvate dallo Stato membro di riferimento (RMS), con procedura FR/H/0797/II/018/G, relativamente al medicinale RADELUMIN:

tipo II, B.I.a.1 - modifica del fabbricante di una materia prima, di un reattivo o di un prodotto intermedio utilizzati nel procedimento di fabbricazione di un principio attivo o modifica del fabbricante del principio attivo (compresi eventualmente i siti di controllo della qualità), per i quali non si dispone di un certificato di conformità alla farmacopea europea; *g)* introduzione di un nuovo fabbricante del principio attivo che non ha il sostegno di un ASMF e che richiede un aggiornamento significativo della pertinente sezione del fascicolo del principio attivo;

tipo IA_{IN}, B.II.b.2 - modifiche a livello di importatore, di modalità di rilascio dei lotti e di prove di controllo qualitativo del prodotto finito; *c)* sostituzione o aggiunta di un fabbricante responsabile dell'importazione e/o del rilascio dei lotti; 2. compresi il controllo dei lotti/le prove:

Advanced Accelerator Applications Molecular Imaging France S.A.S Saint Cloud, 3 rue Charles Lauer, 92210 Saint-Cloud, France;

tipo IA_{IN}, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *a)* sito di confezionamento secondario.

tipo II, B.II.b.1 - sostituzione o aggiunta di un sito di fabbricazione per una parte o per la totalità del procedimento di fabbricazione del prodotto finito; *c)* sito in cui sono effettuate tutte le operazioni di fabbricazione, ad eccezione del rilascio dei lotti, del controllo dei lotti e del confezionamento secondario, o destinato alle forme farmaceutiche prodotte attraverso procedimenti di fabbricazione complessi.

Si modificano gli stampati, paragrafo 6 del foglio illustrativo, come descritto:

6. Contenuto della confezione e altre informazioni

[…]

Produttori:

[…]

AAA Molecular Imaging France S.A.S. Saint Cloud, 3 Rue Charles Lauer, 92210 Saint-Cloud, Francia.

Confezioni A.I.C. n.:

050594047 - «2000 mbq/ml soluzione iniettabile» 1 flaconcino multidose in vetro da 10 ml contenente da 0,3 ml a 10 ml;

050594050 - «2000 mbq/ml soluzione iniettabile» 1 flaconcino multidose in vetro da 15 ml contenente da 0,3 ml a 15 ml;

050594062 - «2000 mbq/ml soluzione iniettabile» 1 flaconcino multidose in vetro da 20 ml contenente da 0,3 ml a 20 ml.

Titolare A.I.C.: ABX advanced biochemical compounds - Biomedizinische Forschungsreagenzien GmbH, con sede legale e domicilio fiscale in Heinrich-Gläser-Straße 10-14, 01454 Radeberg, Germania.

Procedure europee: FR/H/0797/II/013/G - FR/H/0797/II/018/G.

Codici pratica: VC2/2023/306 - VC2/2023/455.

Stampati

Le confezioni del medicinale devono essere poste in commercio con gli stampati, così come precedentemente autorizzati da questa amministrazione, con le sole modifiche necessarie per l'adeguamento alla presente determina.

Il titolare dell'autorizzazione all'immissione in commercio deve apportare le modifiche autorizzate, dalla data di entrata in vigore della determina, di cui al presente estratto, al riassunto delle caratteristiche del prodotto; entro e non oltre i sei mesi dalla medesima data al foglio illustrativo.

In ottemperanza all'art. 80, commi 1 e 3, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, il foglio illustrativo deve essere redatto in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Smaltimento scorte

Sia i lotti già prodotti alla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto che i lotti prodotti nel periodo di cui al precedente paragrafo del presente estratto, che non riportino le modifiche autorizzate, possono essere mantenuti in commercio fino alla data di scadenza del medicinale indicata in etichetta, ai sensi dell'art. 1, comma 7 della determina AIFA n. DG/821/2018 del 24 maggio 2018, pubblicata nella *Gazzetta Ufficiale* della Repubblica italiana n. 133 dell'11 giugno 2018.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05054

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di acido folico, «Acido folico Aristo».

Estratto determina AAM/PPA n. 742/2024 del 20 settembre 2024

È autorizzata l'immissione in commercio del medicinale ACIDO FOLICO ARISTO, anche nella forma farmaceutica, dosaggio e confezione di seguito indicata:

confezione: «5 mg compresse» 84 compresse in blister PVC/PVDC/PVC/Al - A.I.C. n. 048957070 (base 10) 1GQ1NG (base 32).

Principio attivo: acido folico.

Titolare A.I.C.: Aristo Pharma GmbH, con sede legale e domicilio fiscale in Wallenroder Straße 8-10, 13435 Berlino, Germania.

Procedura europea: DE/H/8095/001/IA/005.

Codice pratica: C1A/2024/1737.

Classificazione ai fini della rimborsabilità

Per la nuova confezione sopracitata è adottata la seguente classificazione ai fini della rimborsabilità: C(nn).

Classificazione ai fini della fornitura

Per la nuova confezione sopracitata è adottata la seguente classificazione ai fini della fornitura: RR (medicinali soggetti a prescrizione medica).

Stampati

Le confezioni del medicinale devono essere poste in commercio con gli stampati, così come precedentemente autorizzati da questa amministrazione, con le sole modifiche necessarie per l'adeguamento alla presente determina.

In ottemperanza all'art. 80, commi 1 e 3 del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni il foglio illustrativo e le etichette devono essere redatti in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05055

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di itraconazolo, «Itragerm».

Estratto determina AAM/PPA n. 743/2024 del 20 settembre 2024

L'autorizzazione all'immissione in commercio è modificata, a seguito della seguente variazione, approvata dallo Stato membro di riferimento (RMS), relativamente al medicinale ITRAGERM:

Tipo II, C.I.2b) - Aggiornamento degli stampati sulla base di studi clinici, con aggiunta di informazioni riguardanti l'«acidità gastrica»; si modificano i paragrafi 4.4, 4.5, 5.2 del riassunto delle caratteristiche del prodotto e corrispondenti paragrafi del foglio illustrativo.

Confezioni A.I.C. n.:

044757019 - «50 mg capsule rigide» 4 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757021 - «50 mg capsule rigide» 6 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757033 - «50 mg capsule rigide» 7 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757045 - «50 mg capsule rigide» 8 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757058 - «50 mg capsule rigide» 14 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757060 - «50 mg capsule rigide» 15 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757072 - «50 mg capsule rigide» 18 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757084 - «50 mg capsule rigide» 28 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757096 - «50 mg capsule rigide» 30 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757108 - «50 mg capsule rigide» 60 capsule in blister Pvc/Pe/Pvdc/Al (Triplex);

044757110 - «50 mg capsule rigide» 4 capsule in blister Opa/Al/Pvc;

044757122 - «50 mg capsule rigide» 6 capsule in blister Opa/Al/Pvc;

044757134 - «50 mg capsule rigide» 7 capsule in blister Opa/Al/Pvc;

044757146 - «50 mg capsule rigide» 8 capsule in blister Opa/Al/Pvc;

044757159 - «50 mg capsule rigide» 14 capsule in blister Opa/Al/Pvc;

044757161 - «50 mg capsule rigide» 15 capsule in blister Opa/Al/Pvc;

044757173 - «50 mg capsule rigide» 18 capsule in blister Opa/Al/Pvc;

044757185 - «50 mg capsule rigide» 28 capsule in blister Opa/Al/Pvc;

044757197 - «50 mg capsule rigide» 30 capsule in blister Opa/Al/Pvc;

044757209 - «50 mg capsule rigide» 60 capsule in blister Opa/Al/Pvc;

044757211 - «50 mg capsule rigide» 15 capsule in flacone Hdpe;

044757223 - «50 mg capsule rigide» 30 capsule in flacone Hdpe;

044757235 - «50 mg capsule rigide» 60 capsule in flacone Hdpe;

044757247 - «50 mg capsule rigide» 90 capsule in flacone Hdpe.

Gli stampati corretti ed approvati sono allegati alla determina, di cui al presente estratto.

Titolare A.I.C.: Isdin S.r.l., codice fiscale 06115640960, con sede legale e domicilio fiscale in via Statuto n. 4, 20121 Milano, Italia.

Procedura europea: ES/H/0599/001/II/027.

Codice pratica: VC2/2023/600.

Stampati

Il titolare dell'autorizzazione all'immissione in commercio deve apportare le modifiche autorizzate, dalla data di entrata in vigore della determina, di cui al presente estratto, al riassunto delle caratteristiche del prodotto; entro e non oltre i sei mesi dalla medesima data al foglio illustrativo.

In ottemperanza all'art. 80, commi 1 e 3, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, il foglio illustrativo deve essere redatto in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Smaltimento scorte

Sia i lotti già prodotti alla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto che i lotti prodotti nel periodo di cui al precedente paragrafo del presente estratto, che non riportino le modifiche autorizzate, possono essere mantenuti in commercio fino alla data di scadenza del medicinale indicata in etichetta. A decorrere dal termine di trenta giorni dalla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto, i farmacisti sono tenuti a consegnare il foglio illustrativo aggiornato agli utenti, che scelgono la modalità di ritiro in formato cartaceo o analogico o mediante l'utilizzo di metodi digitali alternativi. Il titolare A.I.C. rende accessibile al farmacista il foglio illustrativo aggiornato entro il medesimo termine.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05056

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di citisiniclina «Kobayzaren».

Estratto determina AAM/PPA n. 744/2024 del 20 settembre 2024

Trasferimento di titolarità: AIN/2024/1477.

Cambio nome: N1B/2024/1017.

È autorizzato il trasferimento di titolarità dell'autorizzazione all'immissione in commercio del sotto elencato medicinale fino ad ora registrato a nome della società Alfrapharma S.r.l. con sede legale e domicilio fiscale in viale Manzoni, 59 - 00185 Roma, codice fiscale 07227261000.

Medicinale: KOBAYZAREN.

Confezione: «1,5 mg compresse rivestite con film» 100 compresse in blister PVC/PVDC/AL - A.I.C. n. 049451014.

Alla società Adamed S.r.l. con sede legale e domicilio fiscale in via Giuseppe Mazzini, 20 - 20123 Milano, codice fiscale 10753240968.

Con variazione della denominazione del medicinale in RECIGAR.

Stampati

Il titolare dell'autorizzazione all'immissione in commercio del medicinale sopraindicato deve apportare le necessarie modifiche al riassunto delle caratteristiche del prodotto dalla data di entrata in vigore della determina, di cui al presente estratto; al foglio illustrativo ed alle etichette dal primo lotto di produzione successivo all'entrata in vigore della determina, di cui al presente estratto.

Smaltimento scorte

I lotti del medicinale, già prodotti e rilasciati a nome del precedente titolare alla data di entrata in vigore della determina, di cui al presente estratto, possono essere mantenuti in commercio fino alla data di scadenza indicata in etichetta.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05057

Modifica dell'autorizzazione all'immissione in commercio del medicinale per uso umano, a base di Tiapride cloridrato, «Italprid».

Estratto determina AAM/PPA n. 752/2024 del 20 settembre 2024

È autorizzata la seguente variazione.

Tipo II - C.I.3.b) sono modificati i paragrafi 4.3, 4.4, 4.5, 4.6, 4.8, 4.9, 5.3 del riassunto delle caratteristiche del prodotto.

Modifiche editoriali e di adeguamento al QRD nei paragrafi 4.7, 5.1, 6.5, 6.6 e 8 del riassunto delle caratteristiche del prodotto e modifiche ai paragrafi 2, 3 e 4 del foglio illustrativo.

Sono inoltre aggiornati le etichette in accordo al QRD *template* e l'aggiornamento dei requisiti nazionali per le *Blue Box*.

Relativamente al medicinale ITALPRID nella forma farmaceutica, dosaggio e confezione di seguito indicata:

A.I.C. n. 023913015 - 20 compresse 100 mg.

Codice pratica: VN2/2022/201.

Titolare A.I.C.: Teofarma S.r.l. con sede legale e domicilio fiscale in via Fratelli Cervi, 8 - 27010 Valle Salimbene, Pavia, codice fiscale 01423300183.

Gli stampati corretti e approvati sono allegati alla determina, di cui al presente estratto.

Stampati

1. Il titolare dell'autorizzazione all'immissione in commercio deve apportare le modifiche autorizzate, dalla data di entrata in vigore della determina, di cui al presente estratto, al riassunto delle caratteristiche del prodotto; entro e non oltre i sei mesi dalla medesima data al foglio illustrativo e all'etichettatura.

2. In ottemperanza all'art. 80, commi 1 e 3, del decreto legislativo 24 aprile 2006, n. 219 e successive modificazioni ed integrazioni, il foglio illustrativo e le etichette devono essere redatti in lingua italiana e, limitatamente ai medicinali in commercio nella Provincia di Bolzano, anche in lingua tedesca. Il titolare dell'A.I.C. che intende avvalersi dell'uso complementare di lingue estere, deve darne preventiva comunicazione all'AIFA e tenere a disposizione la traduzione giurata dei testi in lingua tedesca e/o in altra lingua estera. In caso di inosservanza delle disposizioni sull'etichettatura e sul foglio illustrativo si applicano le sanzioni di cui all'art. 82 del suddetto decreto legislativo.

Smaltimento scorte

Sia i lotti già prodotti alla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto che i lotti prodotti nel periodo di cui al precedente paragrafo del presente estratto, che non riportino le modifiche autorizzate, possono essere mantenuti in commercio fino alla data di scadenza del medicinale indicata in etichetta. A decorrere dal termine di trenta giorni dalla data di pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana del presente estratto, i farmacisti sono tenuti a consegnare il foglio illustrativo aggiornato agli utenti, che scelgono la modalità di ritiro in formato cartaceo o analogico o mediante l'utilizzo di metodi digitali alternativi. Il titolare A.I.C. rende accessibile al farmacista il foglio Illustrativo aggiornato entro il medesimo termine.

Decorrenza di efficacia della determina: dal giorno successivo a quello della sua pubblicazione, per estratto, nella *Gazzetta Ufficiale* della Repubblica italiana.

24A05058

Revoca, su rinuncia, dell'autorizzazione all'immissione in commercio di taluni medicinali per uso umano

Con la determina n. aRM - 179/2024 - 1214 del 18 settembre 2024 è stata revocata, ai sensi dell'art. 38, comma 9, del decreto legislativo n. 219/2006, su rinuncia della Weleda Italia S.r.l., l'autorizzazione all'immissione in commercio dei sottoelencati medicinali omeopatici, nelle confezioni indicate:

medicinale: ZINNOBER;

confezione: 045807043;

descrizione: «D6 compresse» 1 flacone in vetro da 180 compresse;

confezione: 045807031;

descrizione: «D6 compresse» 1 flacone in vetro da 80 compresse;

confezione: 045807029;

descrizione: «D20 compresse» 1 flacone in vetro da 180 compresse;

confezione: 045807017;

descrizione: «D20 compresse» 1 flacone in vetro da 80 compresse;

medicinale: CONCHAE;

confezione: 047360019;

descrizione: «D30 polvere orale» 1 flacone in vetro da 20 g;

medicinale: BRYONIA;

confezione: 046134045;

descrizione: «6 DH gocce orali, soluzione» 1 flacone contagocce in vetro da 50 ml;

confezione: 046134033;

descrizione: «6 DH gocce orali, soluzione» 1 flacone contagocce in vetro da 20 ml;

confezione: 046134021;

descrizione: «3 DH gocce orali, soluzione» 1 flacone contagocce in vetro da 50 ml;

confezione: 046134019;

descrizione: «3 DH gocce orali, soluzione» 1 flacone contagocce in vetro da 20 ml.

Qualora nel canale distributivo fossero presenti scorte dei medicinali revocati, in corso di validità, le stesse potranno essere smaltite entro e non oltre centottanta giorni dalla data di pubblicazione della presente determina.

24A05059

Revoca, su rinuncia, dell'autorizzazione all'importazione parallela del medicinale per uso umano «Ananase».

Con determina aRM - 180/2024 - 3912 del 19 settembre 2024 è stata revocata, su rinuncia della Pricetag S.p.a., l'autorizzazione all'importazione delle confezioni dei medicinali per uso umano di seguito riportate, rilasciata con procedura di autorizzazione all'importazione parallela.

Medicinale: ANANASE:

confezione: 045081015;

descrizione: «40 mg compresse rivestite» 20 compresse rivestite.

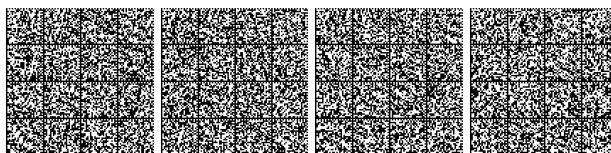
Paese di provenienza: Portogallo.

Qualora nel canale distributivo fossero presenti scorte del medicinale revocato, in corso di validità, le stesse potranno essere smaltite entro e non oltre centottanta giorni dalla data di pubblicazione della presente determina.

24A05060

MINISTERO DELL'AGRICOLTURA, DELLA SOVRANITÀ ALIMENTARE E DELLE FORESTE

Modalità di presentazione e contenuti della domanda di iscrizione di varietà e cloni di vite al Registro nazionale. Abrogazione decreto 30 settembre 2021.

Il decreto ministeriale del 16 luglio 2024, n. 316697, recante le modalità di presentazione e contenuti della domanda di iscrizione di varietà e cloni di vite al registro nazionale, di cui agli articoli 13 e 17 del decreto legislativo 2 febbraio 2021, n. 16. Abrogazione decreto ministeriale 30 settembre 2021, n. 489243, è stato pubblicato sul sito internet del Ministero dell'agricoltura, della sovranità alimentare e delle foreste, alla pagina https://www.politicheagricole.it/flex/cm/pages/ServeBLOB.

php/L/IT/IDPagina/22019 e sul sito internet del Servizio fitosanitario nazionale alla pagina web https://www.protezionedellepiante.it/decreto-ministeriale-del-16-luglio-2024-n-0316697-modalita-di-presentazione-e-contenuti-della-domanda-di-iscrizione-di-varieta-e-cloni-di-vite-al-registro-nazionale-di-cui-agli-artt-13-e-17-del-d/

24A05074

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA

Invito alla manifestazione di interesse per la redazione di pareri sulla verifica della capacità economico-finanziaria degli operatori del settore energetico e/o minerario e per il relativo posizionamento ai fini del rilascio e della gestione dei titoli e delle autorizzazioni conferite nei predetti settori.

Si avvisa che la Direzione generale fonti energetiche e titoli abilitativi del Ministero dell'ambiente e della sicurezza energetica in data 23 settembre 2024 ha approvato l'avviso esplorativo per l'acquisizione di manifestazioni di interesse di soggetti qualificati alla redazione di pareri sulla verifica della capacità economico-finanziaria - CTE - degli operatori del settore energetico e/o minerario e per il relativo posizionamento ai fini del rilascio e della gestione dei titoli e delle autorizzazioni conferite nel predetto settore.

L'invito integrale alla manifestazione di interesse in epigrafe riportata, nella sua stesura completa, è pubblicato sul sito web del citato Ministero (https://unmig.mase.gov.it/).

24A05075

MINISTERO DELLE IMPRESE E DEL MADE IN ITALY

Ripartizione delle risorse residue disponibili in attuazione dell'articolo 6, comma 2, del decreto 3 giugno 2024, per il riconoscimento, per l'anno 2024, del contributo per l'installazione di impianti nuovi a GPL o a metano per l'autotrazione su veicoli di categoria M1 omologati.

Con decreto del direttore generale per la politica industriale, la riconversione e la crisi industriale, l'innovazione, le PMI e il made in Italy del 23 settembre 2024, le risorse di cui al comma 1, art. 4, del decreto direttoriale del 3 giugno 2024, sono state ripartite riservando una quota pari al 30% (trenta per cento) alla concessione dei contributi per l'installazione di impianti nuovi di alimentazione a metano e una quota pari al 70% (settanta per cento) alla concessione dei contributi per l'installazione di impianti nuovi di alimentazione a GPL.

Il decreto è stato emanato in attuazione dell'art. 6, comma 2, del decreto direttoriale del 3 giugno 2024, sulla base del monitoraggio della misura al 15 settembre 2024.

Ai sensi dell'art. 32 della legge 18 giugno 2009, n. 69, il testo integrale del decreto direttoriale è pubblicato e consultabile sul sito del Ministero delle imprese e del made in Italy all'indirizzo https://www.mimit.gov.it

24A05100

MARGHERITA CARDONA ALBINI, *redattore* DELIA CHIARA, *vice redattore*

(WI-GU-2024-GU1-230) Roma, 2024 - Istituto Poligrafico e Zecca dello Stato S.p.A.

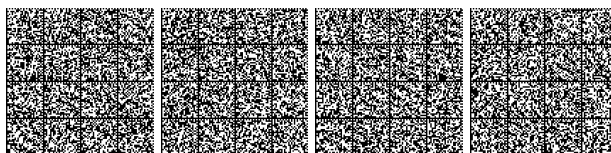
MODALITÀ PER LA VENDITA

La «Gazzetta Ufficiale» e tutte le altre pubblicazioni dell'Istituto sono in vendita al pubblico:

- **— presso il punto vendita dell'Istituto in piazza G. Verdi, 1 - 00198 Roma ☎ 06-8549866**
- **— presso le librerie concessionarie riportate nell'elenco consultabile sui siti www.ipzs.it e www.gazzettaufficiale.it**

L'Istituto conserva per la vendita le Gazzette degli ultimi 4 anni fino ad esaurimento. Le richieste per corrispondenza potranno essere inviate a:

Istituto Poligrafico e Zecca dello Stato S.p.A.
Vendita Gazzetta Ufficiale
Via Salaria, 691
00138 Roma
fax: 06-8508-3466
e-mail: informazioni@gazzettaufficiale.it

avendo cura di specificare nell'ordine, oltre al fascicolo di GU richiesto, l'indirizzo di spedizione e di fatturazione (se diverso) ed indicando i dati fiscali (codice fiscale e partita IVA, se titolari) obbligatori secondo il DL 223/2007. L'importo della fornitura, maggiorato di un contributo per le spese di spedizione, sarà versato in contanti alla ricezione.

DELLA REPUBBLICA ITALIANA

CANONI DI ABBONAMENTO (salvo conguaglio)
validi a partire dal 1° GENNAIO 2024

GAZZETTA UFFICIALE – PARTE I (legislativa)

CANONE DI ABBONAMENTO				
Tipo A	Abbonamento ai fascicoli della Serie Generale, inclusi tutti i supplementi ordinari:			
	(*di cui spese di spedizione € 257,04)**	- annuale	**€**	**438,00**
	(*di cui spese di spedizione € 128,52*) *	- semestrale	**€**	**239,00**
Tipo B	Abbonamento ai fascicoli della 1ª Serie Speciale destinata agli atti dei giudizi davanti alla Corte Costituzionale:			
	(*di cui spese di spedizione € 19,29*)*	- annuale	**€**	**68,00**
	(*di cui spese di spedizione € 9,64*)*	- semestrale	**€**	**43,00**
Tipo C	Abbonamento ai fascicoli della 2ª Serie Speciale destinata agli atti della UE:			
	(*di cui spese di spedizione € 41,27*)*	- annuale	**€**	**168,00**
	(*di cui spese di spedizione € 20,63*)*	- semestrale	**€**	**91,00**
Tipo D	Abbonamento ai fascicoli della 3ª Serie Speciale destinata alle leggi e regolamenti regionali:			
	(*di cui spese di spedizione € 15,31*)*	- annuale	**€**	**65,00**
	(*di cui spese di spedizione € 7,65*)*	- semestrale	**€**	**40,00**
Tipo E	Abbonamento ai fascicoli della 4ª serie speciale destinata ai concorsi indetti dallo Stato e dalle altre pubbliche amministrazioni:			
	(*di cui spese di spedizione € 50,02*)*	- annuale	**€**	**167,00**
	(*di cui spese di spedizione € 25,01*)*	- semestrale	**€**	**90,00**
Tipo F	Abbonamento ai fascicoli della Serie Generale, inclusi tutti i supplementi ordinari, ed ai fascicoli delle quattro serie speciali:			
	(*di cui spese di spedizione € 383,93*)*	- annuale	**€**	**819,00**
	(*di cui spese di spedizione € 191,46*)*	- semestrale	**€**	**431,00**

N.B.: L'abbonamento alla GURI tipo A ed F comprende gli indici mensili

PREZZI DI VENDITA A FASCICOLI (oltre le spese di spedizione)

Prezzi di vendita: serie generale	€	1,00
serie speciali (escluso concorsi), ogni 16 pagine o frazione	€	1,00
fascicolo serie speciale, *concorsi*, prezzo unico	€	1,50
supplementi (ordinari e straordinari), ogni 16 pagine o frazione	€	1,00

I.V.A. 4% a carico dell'Editore

GAZZETTA UFFICIALE - PARTE II

(*di cui spese di spedizione € 40,05*)*	- annuale	**€**	**86,72**
(*di cui spese di spedizione € 20,95*)*	- semestrale	**€**	**55,46**

Prezzo di vendita di un fascicolo, ogni 16 pagine o frazione (oltre le spese di spedizione) € 1,01 (€ 0,83+IVA)

Sulle pubblicazioni della Parte II viene imposta I.V.A. al 22%. Si ricorda che in applicazione della legge 190 del 23 dicembre 2014 articolo 1 comma 629, gli enti dello Stato ivi specificati sono tenuti a versare all'Istituto solo la quota imponibile relativa al canone di abbonamento sottoscritto. Per ulteriori informazioni contattare la casella di posta elettronica editoria@ipzs.it.

RACCOLTA UFFICIALE DEGLI ATTI NORMATIVI

Abbonamento annuo	**€**	**190,00**
Abbonamento annuo per regioni, province e comuni – SCONTO 5%	**€**	**180,50**
Volume separato (oltre le spese di spedizione)	€	18,00

I.V.A. 4% a carico dell'Editore

Per l'estero, i prezzi di vendita (in abbonamento ed a fascicoli separati) anche per le annate arretrate, compresi i fascicoli dei supplementi ordinari e straordinari, devono intendersi raddoppiati. Per il territorio nazionale, i prezzi di vendita dei fascicoli separati, compresi i supplementi ordinari e straordinari, relativi anche ad anni precedenti, devono intendersi raddoppiati. Per intere annate è raddoppiato il prezzo dell'abbonamento in corso.
Le spese di spedizione relative alle richieste di invio per corrispondenza di singoli fascicoli vengono stabilite di volta in volta in base alle copie richieste.
Eventuali fascicoli non recapitati potranno essere forniti gratuitamente entro 60 giorni dalla data di pubblicazione del fascicolo. Oltre tale periodo questi potranno essere forniti soltanto a pagamento.

N.B. – La spedizione dei fascicoli inizierà entro 15 giorni dall'attivazione da parte dell'Ufficio Abbonamenti Gazzetta Ufficiale.
RESTANO CONFERMATI GLI SCONTI COMMERCIALI APPLICATI AI SOLI COSTI DI ABBONAMENTO

* tariffe postali di cui alla Legge 27 febbraio 2004, n. 46 (G.U. n. 48/2004) per soggetti iscritti al R.O.C